

TigerSwitch 10/100

24-Port Layer 3 Switch

- ◆ 24 10BASE-T/100BASE-TX auto-MDI/MDI-X ports
- ◆ Optional 1000BASE-T or 1000BASE-X GBIC modules
- ◆ 8.8 Gbps aggregate bandwidth
- ◆ Non-blocking switching architecture
- ◆ Support for redundant power unit
- ◆ Rapid Spanning Tree Protocol
- ◆ Supports up to 6 static or dynamic trunks
- ◆ Layer 2/3/4 CoS support through four priority queues
- ◆ Full support for VLANs with GVRP
- ◆ IGMP multicast filtering and snooping
- ◆ Layer 3 routing for unicast and multicast traffic
- ◆ Authentication via RADIUS, ACLs, or IEEE 802.1x
- ◆ Manageable via console, Web, SNMP/RMON



TigerSwitch 10/100 Management Guide

From SMC's Tiger line of feature-rich workgroup LAN solutions



38 Tesla
Irvine, CA 92618
Phone: (949) 679-8000

October 2003
Pub. # 150200033700A

Information furnished by SMC Networks, Inc. (SMC) is believed to be accurate and reliable. However, no responsibility is assumed by SMC for its use, nor for any infringements of patents or other rights of third parties which may result from its use. No license is granted by implication or otherwise under any patent or patent rights of SMC. SMC reserves the right to change specifications at any time without notice.

Copyright © 2003 by
SMC Networks, Inc.

38 Tesla

Irvine, CA 92618

All rights reserved. Printed in Taiwan

Trademarks:

SMC is a registered trademark; and TigerSwitch is a trademark of SMC Networks, Inc. Other product and company names are trademarks or registered trademarks of their respective holders.

LIMITED WARRANTY

Limited Warranty Statement: SMC Networks, Inc. (“SMC”) warrants its products to be free from defects in workmanship and materials, under normal use and service, for the applicable warranty term. All SMC products carry a standard 90-day limited warranty from the date of purchase from SMC or its Authorized Reseller. SMC may, at its own discretion, repair or replace any product not operating as warranted with a similar or functionally equivalent product, during the applicable warranty term. SMC will endeavor to repair or replace any product returned under warranty within 30 days of receipt of the product.

The standard limited warranty can be upgraded to a Limited Lifetime* warranty by registering new products within 30 days of purchase from SMC or its Authorized Reseller. Registration can be accomplished via the enclosed product registration card or online via the SMC web site. Failure to register will not affect the standard limited warranty. The Limited Lifetime warranty covers a product during the Life of that Product, which is defined as the period of time during which the product is an “Active” SMC product. A product is considered to be “Active” while it is listed on the current SMC price list. As new technologies emerge, older technologies become obsolete and SMC will, at its discretion, replace an older product in its product line with one that incorporates these newer technologies. At that point, the obsolete product is discontinued and is no longer an “Active” SMC product. A list of discontinued products with their respective dates of discontinuance can be found at:

http://www.smc.com/index.cfm?action=customer_service_warranty.

All products that are replaced become the property of SMC. Replacement products may be either new or reconditioned. Any replaced or repaired product carries either a 30-day limited warranty or the remainder of the initial warranty, whichever is longer. SMC is not responsible for any custom software or firmware, configuration information, or memory data of Customer contained in, stored on, or integrated with any products returned to SMC pursuant to any warranty. Products returned to SMC should have any customer-installed accessory or add-on components, such as expansion modules, removed prior to returning the product for replacement. SMC is not responsible for these items if they are returned with the product.

Customers must contact SMC for a Return Material Authorization number prior to returning any product to SMC. Proof of purchase may be required. Any product returned to SMC without a valid Return Material Authorization (RMA) number clearly marked on the outside of the package will be returned to customer at customer's expense. For warranty claims within North America, please call our toll-free customer support number at (800) 762-4968. Customers are responsible for all shipping charges from their facility to SMC. SMC is responsible for return shipping charges from SMC to customer.

WARRANTIES EXCLUSIVE: IF AN SMC PRODUCT DOES NOT OPERATE AS WARRANTED ABOVE, CUSTOMER'S SOLE REMEDY SHALL BE REPAIR OR REPLACEMENT OF THE PRODUCT IN QUESTION, AT SMC'S OPTION. THE FOREGOING WARRANTIES AND REMEDIES ARE EXCLUSIVE AND ARE IN LIEU OF ALL OTHER WARRANTIES OR CONDITIONS, EXPRESS OR IMPLIED, EITHER IN FACT OR BY OPERATION OF LAW, STATUTORY OR OTHERWISE, INCLUDING WARRANTIES OR CONDITIONS OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. SMC NEITHER ASSUMES NOR AUTHORIZES ANY OTHER PERSON TO ASSUME FOR IT ANY OTHER LIABILITY IN CONNECTION WITH THE SALE, INSTALLATION, MAINTENANCE OR USE OF ITS PRODUCTS. SMC SHALL NOT BE LIABLE UNDER THIS WARRANTY IF ITS TESTING AND EXAMINATION DISCLOSE THE ALLEGED DEFECT IN THE PRODUCT DOES NOT EXIST OR WAS CAUSED BY CUSTOMER'S OR ANY THIRD PERSON'S MISUSE, NEGLIGENCE, IMPROPER INSTALLATION OR TESTING, UNAUTHORIZED ATTEMPTS TO REPAIR, OR ANY OTHER CAUSE BEYOND THE RANGE OF THE INTENDED USE, OR BY ACCIDENT, FIRE, LIGHTNING, OR OTHER HAZARD.

LIMITATION OF LIABILITY: IN NO EVENT, WHETHER BASED IN CONTRACT OR TORT (INCLUDING NEGLIGENCE), SHALL SMC BE LIABLE FOR INCIDENTAL, CONSEQUENTIAL, INDIRECT, SPECIAL, OR PUNITIVE DAMAGES OF ANY KIND, OR FOR LOSS OF REVENUE, LOSS OF BUSINESS, OR OTHER FINANCIAL LOSS ARISING OUT OF OR IN CONNECTION WITH THE SALE, INSTALLATION, MAINTENANCE, USE, PERFORMANCE, FAILURE, OR INTERRUPTION OF ITS PRODUCTS, EVEN IF SMC OR ITS AUTHORIZED RESELLER HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

SOME STATES DO NOT ALLOW THE EXCLUSION OF IMPLIED WARRANTIES OR THE LIMITATION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES FOR CONSUMER PRODUCTS, SO THE ABOVE LIMITATIONS AND EXCLUSIONS MAY NOT APPLY TO YOU. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS, WHICH MAY VARY FROM STATE TO STATE. NOTHING IN THIS WARRANTY SHALL BE TAKEN TO AFFECT YOUR STATUTORY RIGHTS.

* SMC will provide warranty service for one year following discontinuance from the active SMC price list. Under the limited lifetime warranty, internal and external power supplies, fans, and cables are covered by a standard one-year warranty from date of purchase.

SMC Networks, Inc.
38 Tesla
Irvine, CA 92618

CONTENTS

1	Introduction	1-1
	Key Features	1-1
	Description of Software Features	1-2
	System Defaults	1-8
2	Initial Configuration	2-1
	Connecting to the Switch	2-1
	Configuration Options	2-1
	Required Connections	2-2
	Remote Connections	2-4
	Basic Configuration	2-5
	Console Connection	2-5
	Setting Passwords	2-6
	Setting an IP Address	2-6
	Manual Configuration	2-7
	Dynamic Configuration	2-8
	Enabling SNMP Management Access	2-9
	Community Strings	2-9
	Trap Receivers	2-11
	Saving Configuration Settings	2-11
	Managing System Files	2-12
3	Configuring the Switch	3-1
	Using the Web Interface	3-1
	Navigating the Web Browser Interface	3-3
	Home Page	3-3
	Configuration Options	3-4
	Panel Display	3-4
	Main Menu	3-5
	Basic Configuration	3-12
	Displaying System Information	3-12
	Displaying Switch Hardware/Software Versions	3-14
	Displaying Bridge Extension Capabilities	3-16
	Setting the Switch's IP Address	3-17
	Manual Configuration	3-19

Using DHCP/BOOTP	3-20
Managing Firmware	3-22
Downloading System Software from a Server	3-22
Saving or Restoring Configuration Settings	3-23
Downloading Configuration Settings from a Server	3-24
Setting the System Clock	3-25
Configuring SNTP	3-26
Setting the Time Zone	3-27
Resetting the System	3-28
User Authentication	3-28
Configuring the Logon Password	3-28
Configuring Local/Remote Logon Authentication	3-30
Configuring 802.1x Port Authentication	3-32
Displaying 802.1x Global Settings	3-34
Configuring 802.1x Global Settings	3-36
Configuring Port Authorization Mode	3-38
Displaying 802.1x Statistics	3-39
Access Control Lists	3-41
Configuring Access Control Lists	3-41
Setting the ACL Name and Type	3-42
Configuring a Standard IP ACL	3-43
Configuring an Extended IP ACL	3-44
Configuring a MAC ACL	3-47
Binding a Port to an Access Control List	3-49
Simple Network Management Protocol	3-50
Setting Community Access Strings	3-50
Specifying Trap Managers and Trap Types	3-51
Dynamic Host Configuration Protocol	3-53
Configuring DHCP Relay Service	3-53
Configuring the DHCP Server	3-55
Enabling the Server, Setting Excluded Addresses	3-56
Configuring Address Pools	3-57
Displaying Address Bindings	3-62
Port Configuration	3-63
Displaying Connection Status	3-63
Configuring Interface Connections	3-67
Setting Broadcast Storm Thresholds	3-69

Configuring Port Mirroring	3-70
Showing Port Statistics	3-71
Configuring Rate Limits	3-77
Trunk Configuration	3-79
Dynamically Configuring a Trunk	3-80
Statically Configuring a Trunk	3-82
Address Table Settings	3-84
Setting Static Addresses	3-84
Displaying the Address Table	3-85
Changing the Aging Time	3-87
Spanning Tree Algorithm Configuration	3-87
Displaying Global Settings	3-89
Configuring Global Settings	3-92
Displaying Interface Settings	3-95
Configuring Interface Settings	3-99
VLAN Configuration	3-102
Overview	3-102
Assigning Ports to VLANs	3-103
Forwarding Tagged/Untagged Frames	3-106
Enabling or Disabling GVRP (Global Setting)	3-107
Displaying Basic VLAN Information	3-107
Displaying Current VLANs	3-108
Creating VLANs	3-110
Adding Static Members to VLANs (VLAN Index)	3-111
Adding Static Members to VLANs (Port Index)	3-113
Configuring VLAN Behavior for Interfaces	3-114
Configuring Private VLANs	3-118
Enabling Private VLANs	3-118
Configuring Uplink and Downlink Ports	3-119
Class of Service Configuration	3-120
Setting the Default Priority for Interfaces	3-120
Mapping CoS Values to Egress Queues	3-122
Setting the Service Weight for Traffic Classes	3-124
Mapping Layer 3/4 Priorities to CoS Values	3-125
Selecting IP Precedence/DSCP Priority	3-126
Mapping IP Precedence	3-127
Mapping DSCP Priority	3-129

CONTENTS

Mapping IP Port Priority	3-131
Copying IP Settings to Another Interface	3-133
Multicast Filtering	3-134
IGMP Protocol	3-135
Layer 2 IGMP (Snooping and Query)	3-136
Configuring IGMP Snooping Parameters	3-137
Displaying Interfaces Attached to a Multicast Router ..	3-139
Specifying Static Interfaces for a Multicast Router	3-140
Displaying Port Members of Multicast Services	3-142
Assigning Ports to Multicast Services	3-143
Layer 3 IGMP (Query used with Multicast Routing)	3-144
Configuring IGMP Interface Parameters	3-145
Displaying Multicast Group Information	3-148
IP Routing	3-149
Overview	3-149
Initial Configuration	3-150
IP Switching	3-151
Routing Path Management	3-152
Routing Protocols	3-152
Basic IP Interface Configuration	3-154
Configuring IP Routing Interfaces	3-155
Address Resolution Protocol	3-157
Proxy ARP	3-158
Basic ARP Configuration	3-159
Configuring Static ARP Addresses	3-160
Displaying Dynamically Learned ARP Entries	3-161
Displaying Local ARP Entries	3-163
Displaying ARP Statistics	3-164
Displaying Statistics for IP Protocols	3-165
IP Statistics	3-165
ICMP Statistics	3-168
UDP Statistics	3-170
TCP Statistics	3-171
Configuring Static Routes	3-172
Displaying the Routing Table	3-173
Configuring the Routing Information Protocol	3-175
Configuring General Protocol Settings	3-176

Specifying Network Interfaces for RIP	3-178
Configuring Network Interfaces for RIP	3-179
Displaying RIP Information and Statistics	3-183
Configuring the Open Shortest Path First Protocol	3-186
Configuring General Protocol Settings	3-188
Configuring OSPF Areas	3-192
Configuring Area Ranges (Route Summarization for ABRs)	3-196
Configuring OSPF Interfaces	3-198
Configuring Virtual Links	3-204
Configuring Network Area Addresses	3-206
Configuring Summary Addresses (for External AS Routes)	3-208
Redistributing External Routes	3-210
Configuring NSSA Settings	3-212
Displaying Link State Database Information	3-213
Displaying Information on Border Routers	3-216
Displaying Information on Neighbor Routers	3-217
Multicast Routing	3-218
Configuring Global Settings for Multicast Routing	3-219
Displaying the Multicast Routing Table	3-219
Configuring DVMRP	3-222
Configuring Global DVMRP Settings	3-223
Configuring DVMRP Interface Settings	3-227
Displaying Neighbor Information	3-229
Displaying the Routing Table	3-230
Configuring PIM-DM	3-231
Configuring Global PIM-DM Settings	3-232
Configuring PIM-DM Interface Settings	3-233
Displaying Interface Information	3-236
Displaying Neighbor Information	3-237
4 Command Line Interface	4-1
Using the Command Line Interface	4-1
Accessing the CLI	4-1
Console Connection	4-1
Telnet Connection	4-2
Entering Commands	4-3
Keywords and Arguments	4-3

CONTENTS

Minimum Abbreviation	4-4
Command Completion	4-4
Getting Help on Commands	4-4
Showing Commands	4-5
Partial Keyword Lookup	4-6
Negating the Effect of Commands	4-6
Using Command History	4-6
Understanding Command Modes	4-6
Exec Commands	4-7
Configuration Commands	4-8
Command Line Processing	4-10
Command Groups	4-11
Line Commands	4-13
line	4-14
login	4-15
password	4-16
exec-timeout	4-17
password-thresh	4-18
silent-time	4-19
databits	4-20
parity	4-21
speed	4-22
stopbits	4-23
show line	4-23
General Commands	4-24
enable	4-25
disable	4-26
configure	4-27
show history	4-27
reload	4-28
end	4-29
exit	4-29
quit	4-30
System Management Commands	4-31
Device Designation Commands	4-31
hostname	4-32
User Access Commands	4-32

username	4-33
enable password	4-34
Web Server Commands	4-35
ip http port	4-35
ip http server	4-36
Event Logging Commands	4-37
logging on	4-37
logging history	4-38
clear logging	4-39
show logging	4-40
Time Commands	4-41
snmp client	4-42
snmp server	4-43
snmp poll	4-44
snmp broadcast client	4-45
show snmp	4-45
clock timezone	4-46
System Status Commands	4-47
show startup-config	4-47
show running-config	4-49
show system	4-51
show users	4-51
show version	4-52
Flash/File Commands	4-53
copy	4-53
delete	4-56
dir	4-57
whichboot	4-58
boot system	4-59
Authentication Commands	4-60
Authentication Sequence	4-60
authentication login	4-60
RADIUS Client	4-61
radius-server host	4-62
radius-server port	4-63
radius-server key	4-63
radius-server retransmit	4-64

CONTENTS

radius-server timeout	4-65
show radius-server	4-65
802.1x Port Authentication	4-66
authentication dot1x default	4-67
dot1x default	4-67
dot1x max-req	4-68
dot1x port-control	4-68
dot1x re-authenticate	4-69
dot1x re-authentication	4-69
dot1x timeout quiet-period	4-70
dot1x timeout re-authperiod	4-70
dot1x timeout tx-period	4-71
show dot1x	4-72
Access Control List Commands	4-74
IP ACLs	4-76
access-list ip	4-76
permit, deny (Standard ACL)	4-78
permit, deny (Extended ACL)	4-79
ip access-group	4-81
show ip access-group	4-82
show ip access-list	4-83
MAC ACLs	4-84
access-list mac	4-84
permit, deny (MAC ACL)	4-85
mac access-group	4-87
show mac access-group	4-87
show mac access-list	4-88
ACL Information	4-89
show access-list	4-89
show access-group	4-89
SNMP Commands	4-90
snmp-server community	4-90
snmp-server contact	4-91
snmp-server location	4-92
snmp-server host	4-93
snmp-server enable traps	4-94
show snmp	4-95

DHCP Commands	4-97
DHCP Client	4-97
ip dhcp client-identifier	4-97
ip dhcp restart client	4-98
DHCP Relay	4-99
ip dhcp restart relay	4-99
ip dhcp relay server	4-101
DHCP Server	4-102
service dhcp	4-103
ip dhcp excluded-address	4-104
ip dhcp pool	4-104
network	4-105
default-router	4-106
domain-name	4-107
dns-server	4-108
next-server	4-109
bootfile	4-109
netbios-name-server	4-110
netbios-node-type	4-111
lease	4-112
host	4-113
client-identifier	4-114
hardware-address	4-115
clear ip dhcp binding	4-116
show ip dhcp binding	4-117
Interface Commands	4-118
interface	4-119
description	4-119
speed-duplex	4-120
negotiation	4-121
capabilities	4-122
flowcontrol	4-124
shutdown	4-125
switchport broadcast packet-rate	4-126
clear counters	4-127
show interfaces status	4-128
show interfaces counters	4-129

show interfaces switchport	4-131
Mirror Port Commands	4-133
port monitor	4-133
show port monitor	4-134
Rate Limit Commands	4-135
rate-limit	4-136
Link Aggregation Commands	4-137
channel-group	4-138
lacp	4-139
Address Table Commands	4-141
mac-address-table static	4-141
clear mac-address-table dynamic	4-142
show mac-address-table	4-143
mac-address-table aging-time	4-144
show mac-address-table aging-time	4-145
Spanning Tree Commands	4-146
spanning-tree	4-147
spanning-tree mode	4-148
spanning-tree forward-time	4-149
spanning-tree hello-time	4-150
spanning-tree max-age	4-150
spanning-tree priority	4-151
spanning-tree pathcost method	4-152
spanning-tree transmission-limit	4-153
spanning-tree cost	4-154
spanning-tree port-priority	4-155
spanning-tree edge-port	4-156
spanning-tree portfast	4-157
spanning-tree link-type	4-158
spanning-tree protocol-migration	4-159
show spanning-tree	4-160
VLAN Commands	4-162
Editing VLAN Groups	4-162
vlan database	4-162
vlan	4-163
Configuring VLAN Interfaces	4-164
interface vlan	4-165

switchport mode	4-166
switchport acceptable-frame-types	4-167
switchport ingress-filtering	4-168
switchport native vlan	4-169
switchport allowed vlan	4-170
switchport forbidden vlan	4-171
Displaying VLAN Information	4-172
show vlan	4-172
Configuring Private VLANs	4-173
pvlan	4-173
show pvlan	4-174
GVRP and Bridge Extension Commands	4-175
bridge-ext gvrp	4-175
show bridge-ext	4-176
switchport gvrp	4-177
show gvrp configuration	4-178
garp timer	4-178
show garp timer	4-180
Priority Commands	4-181
Priority Commands (Layer 2)	4-181
switchport priority default	4-182
queue bandwidth	4-183
queue cos-map	4-184
show queue bandwidth	4-185
show queue cos-map	4-186
Priority Commands (Layer 3 and 4)	4-187
map ip port (Global Configuration)	4-187
map ip port (Interface Configuration)	4-188
map ip precedence (Global Configuration)	4-189
map ip precedence (Interface Configuration)	4-189
map ip dscp (Global Configuration)	4-191
map ip dscp (Interface Configuration)	4-191
show map ip port	4-193
show map ip precedence	4-194
show map ip dscp	4-195
Multicast Filtering Commands	4-196
IGMP Snooping Commands	4-196

ip igmp snooping	4-197
ip igmp snooping vlan static	4-197
ip igmp snooping version	4-198
show ip igmp snooping	4-199
show mac-address-table multicast	4-200
IGMP Query Commands (Layer 2)	4-201
ip igmp snooping querier	4-201
ip igmp snooping query-count	4-202
ip igmp snooping query-interval	4-203
ip igmp snooping query-max-response-time	4-203
ip igmp snooping router-port-expire-time	4-204
IGMP Commands (Layer 3)	4-205
ip igmp	4-206
ip igmp robustval	4-207
ip igmp query-interval	4-207
ip igmp max-resp-interval	4-208
ip igmp last-memb-query-interval	4-209
ip igmp version	4-210
show ip igmp interface	4-211
clear ip igmp group	4-212
show ip igmp groups	4-213
IP Interface Commands	4-215
Basic IP Configuration	4-215
ip address	4-216
ip default-gateway	4-218
show ip interface	4-219
show ip redirects	4-219
ping	4-220
Address Resolution Protocol (ARP)	4-221
arp	4-222
arp-timeout	4-223
clear arp-cache	4-223
show arp	4-224
ip proxy-arp	4-224
IP Routing Commands	4-225
Global Routing Configuration	4-226
ip routing	4-226

ip route	4-227
clear ip route	4-228
show ip route	4-228
show ip traffic	4-229
Routing Information Protocol (RIP)	4-231
router rip	4-231
timers basic	4-232
network	4-233
neighbor	4-234
version	4-235
ip rip receive version	4-236
ip rip send version	4-237
ip split-horizon	4-239
ip rip authentication key	4-240
ip rip authentication mode	4-241
show rip globals	4-242
show ip rip	4-242
Open Shortest Path First (OSPF)	4-244
router ospf	4-246
router-id	4-247
compatible rfc1583	4-248
default-information originate	4-248
timers spf	4-250
area range	4-251
area default-cost	4-252
summary-address	4-253
redistribute	4-254
network area	4-255
area stub	4-257
area nssa	4-258
area virtual-link	4-260
ip ospf authentication	4-263
ip ospf authentication-key	4-264
ip ospf message-digest-key	4-265
ip ospf cost	4-266
ip ospf dead-interval	4-267
ip ospf hello-interval	4-268

CONTENTS

ip ospf priority	4-268
ip ospf retransmit-interval	4-269
ip ospf transmit-delay	4-270
show ip ospf	4-271
show ip ospf border-routers	4-272
show ip ospf database	4-273
show ip ospf interface	4-281
show ip ospf neighbor	4-282
show ip ospf summary-address	4-283
show ip ospf virtual-links	4-284
Multicast Routing Commands	4-285
Static Multicast Routing Commands	4-285
ip igmp snooping vlan mrouter	4-286
show ip igmp snooping mrouter	4-287
General Multicast Routing Commands	4-287
ip multicast-routing	4-288
show ip mroute	4-288
DVMRP Multicast Routing Commands	4-290
router dvmrp	4-291
probe-interval	4-292
nbr-timeout	4-293
report-interval	4-293
flash-update-interval	4-294
prune-lifetime	4-294
default-gateway	4-295
ip dvmrp	4-296
ip dvmrp metric	4-297
clear ip dvmrp route	4-298
show router dvmrp	4-298
show ip dvmrp route	4-299
show ip dvmrp neighbor	4-300
show ip dvmrp interface	4-301
PIM-DM Multicast Routing Commands	4-301
router pim	4-302
ip pim dense-mode	4-303
ip pim hello-interval	4-304
ip pim hello-holdtime	4-305

	ip pim trigger-hello-interval	4-305
	ip pim join-prune-holdtime	4-306
	ip pim graft-retry-interval	4-307
	ip pim max-graft-retries	4-308
	show router pim	4-308
	show ip pim interface	4-309
	show ip pim neighbor	4-309
A	Troubleshooting	A-1
B	Upgrading Firmware via the Serial Port	B-1
	Glossary	
	Index	

CONTENTS

CHAPTER 1

INTRODUCTION

This switch provides a broad range of features for Layer 2 switching and Layer 3 routing. It includes a management agent that allows you to configure the features listed in this manual. The default configuration can be used for most of the features provided by this switch. However, there are many options that you should configure to maximize the switch's performance for your particular network environment.

Key Features

Feature	Description
Configuration Backup and Restore	Backup to TFTP server
Authentication	Console, Telnet, Web – User name / password, RADIUS SNMP – Community strings Port – IEEE 802.1x
Access Control Lists	Supports up to 32 IP or MAC ACLs
DHCP Relay and Server	Supported
Port Configuration	Speed, duplex mode and flow control
Rate Limiting	Input and output rate limiting per port
Port Mirroring	One or more ports mirrored to single analysis port
Port Trunking	Supports up to 6 trunks using either static or dynamic trunking (LACP)

Feature	Description
Broadcast Storm Control	Supported
Address Table	Up to 8K MAC addresses in the forwarding table, 100 static MAC addresses per port; Up to 2K IP address entries, 128 static IP addresses in the ARP cache, 256 static IP routes
IEEE 802.1D Bridge	Supports dynamic data switching and addresses learning
Store-and-Forward Switching	Supported to ensure wire-speed switching while eliminating bad frames
Spanning Tree Protocol	Supports standard STP and the new Rapid Spanning Tree Protocol (RSTP)
Virtual LANs	Up to 255 using IEEE 802.1Q, or private VLANs
Traffic Prioritization	Default port priority, traffic class map, queue scheduling, IP Precedence, Differentiated Services Code Point (DSCP), and TCP/UDP Port
IP Routing	Routing Information Protocol (RIP), Open Shortest Path First (OSPF), static routes
ARP	Static and dynamic address configuration, proxy ARP
Multicast Filtering	Supports IGMP snooping and query for Layer 2, and IGMP for Layer 3
Multicast Routing	Supports DVMRP and PIM-DM

Description of Software Features

The switch provides a wide range of advanced performance enhancing features. Flow control eliminates the loss of packets due to bottlenecks caused by port saturation. Broadcast storm suppression prevents broadcast traffic storms from engulfing the network. Port-based VLANs, plus support for automatic GVRP VLAN registration provide traffic security and efficient use of network bandwidth. CoS priority queueing ensures the

minimum delay for moving real-time multimedia data across the network. While multicast filtering and routing provide support for real-time network applications. Some of the management features are briefly described below.

Configuration Backup and Restore – You can save the current configuration settings to a file on a TFTP server, and later download this file to restore the switch configuration settings.

Authentication – This switch authenticates management access via the console port, Telnet or Web browser. User names and passwords can be configured locally or can be verified via a remote authentication server (i.e., RADIUS). Port-based authentication is also supported via the IEEE 802.1x protocol. This protocol uses the Extensible Authentication Protocol over LANs (EAPOL) to request a user name and password from the 802.1x client, and then verifies the client's right to access the network via an authentication server (i.e., RADIUS server).

Access Control Lists – ACLs provide packet filtering for IP frames (based on address, protocol, TCP/UDP port number or TCP control code) or any frames (based on MAC address or Ethernet type). ACLs can be used to improve performance by blocking unnecessary network traffic or to implement security controls by restricting access to specific network resources or protocols.

DHCP Server and DHCP Relay – A DHCP server is provided to assign IP addresses to host devices. Since DHCP uses a broadcast mechanism, a DHCP server and its client must physically reside on the same subnet. Since it is not practical to have a DHCP server on every subnet, DHCP Relay is also supported to allow dynamic configuration of local clients from a DHCP server located in a different network.

Port Configuration – You can manually configure the speed, duplex mode, and flow control used on specific ports, or use auto-negotiation to detect the connection settings used by the attached device. Use the full-duplex mode on ports whenever possible to double the throughput of switch connections. Flow control should also be enabled to control

network traffic during periods of congestion and prevent the loss of packets when port buffer thresholds are exceeded. The switch supports flow control based on the IEEE 802.3x standard.

Rate Limiting – This feature controls the maximum rate for traffic transmitted or received on an interface. Rate limiting is configured on interfaces at the edge of a network to limit traffic into or out of the network. Traffic that falls within the rate limit is transmitted, while packets that exceed the acceptable amount of traffic are dropped.

Port Mirroring – The switch can unobtrusively mirror traffic from any port to a monitor port. You can then attach a protocol analyzer or RMON probe to this port to perform traffic analysis and verify connection integrity.

Port Trunking – Ports can be combined into an aggregate connection. Trunks can be manually set up or dynamically configured using IEEE 802.3ad Link Aggregation Control Protocol (LACP). The additional ports dramatically increase the throughput across any connection, and provide redundancy by taking over the load if a port in the trunk should fail. The switch supports up to six trunks.

Broadcast Storm Control – Broadcast suppression prevents broadcast traffic from overwhelming the network. When enabled on a port, the level of broadcast traffic passing through the port is restricted. If broadcast traffic rises above a pre-defined threshold, it will be throttled until the level falls back beneath the threshold.

Static Addresses – A static address can be assigned to a specific interface on this switch. Static addresses are bound to the assigned interface and will not be moved. When a static address is seen on another interface, the address will be ignored and will not be written to the address table. Static addresses can be used to provide network security by restricting access for a known host to a specific port.

IEEE 802.1D Bridge – The switch supports IEEE 802.1D transparent bridging. The address table facilitates data switching by learning addresses, and then filtering or forwarding traffic based on this information. The address table supports up to 8K addresses.

Store-and-Forward Switching – The switch copies each frame into its memory before forwarding them to another port. This ensures that all frames are a standard Ethernet size and have been verified for accuracy with the cyclic redundancy check (CRC). This prevents bad frames from entering the network and wasting bandwidth.

To avoid dropping frames on congested ports, the switch provides 8 MB for frame buffering. This buffer can queue packets awaiting transmission on congested networks.

Spanning Tree Protocol – The switch supports these spanning tree protocols:

Spanning Tree Protocol (STP, IEEE 802.1D) – This protocol adds a level of fault tolerance by allowing two or more redundant connections to be created between a pair of LAN segments. When there are multiple physical paths between segments, this protocol will choose a single path and disable all others to ensure that only one route exists between any two stations on the network. This prevents the creation of network loops. However, if the chosen path should fail for any reason, an alternate path will be activated to maintain the connection.

Rapid Spanning Tree Protocol (RSTP, IEEE 802.1w) – This protocol reduces the convergence time for network topology changes to about 10% of that required by the older IEEE 802.1D STP standard. It is intended as a complete replacement for STP, but can still interoperate with switches running the older standard by automatically reconfiguring ports to STP-compliant mode if they detect STP protocol messages from attached devices.

Virtual LANs – The switch supports up to 255 VLANs. A Virtual LAN is a collection of network nodes that share the same collision domain regardless of their physical location or connection point in the network. The switch supports tagged VLANs based on the IEEE 802.1Q standard. Members of VLAN groups can be dynamically learned via GVRP, or ports can be manually assigned to a specific set of VLANs. This allows the switch to restrict traffic to the VLAN groups to which a user has been assigned. By segmenting your network into VLANs, you can:

- Eliminate broadcast storms which severely degrade performance in a flat network.
- Simplify network management for node changes/moves by remotely configuring VLAN membership for any port, rather than having to manually change the network connection.
- Provide data security by restricting all traffic to the originating VLAN, except where a connection is explicitly defined via the switch's routing service.
- Use private VLANs to restrict traffic to pass only between data ports and the uplink ports, thereby isolating adjacent ports within the same VLAN, and allowing you to limit the total number of VLANs that need to be configured.

Traffic Prioritization – This switch prioritizes each packet based on the required level of service, using four priority queues with Weighted Round Robin Queuing. It uses IEEE 802.1p and 802.1Q tags to prioritize incoming traffic based on input from the end-station application. These functions can be used to provide independent priorities for delay-sensitive data and best-effort data.

This switch also supports several common methods of prioritizing layer 3/4 traffic to meet application requirements. Traffic can be prioritized based on the priority bits in the IP frame's Type of Service (ToS) octet or the number of the TCP/UDP port. When these services are enabled, the priorities are mapped to a Class of Service value by the switch, and the traffic then sent to the corresponding output queue.

IP Routing – The switch provides Layer 3 IP routing. To maintain a high rate of throughput, the switch forwards all traffic passing within the same segment, and routes only traffic that passes between different subnetworks. The wire-speed routing provided by this switch lets you easily link network segments or VLANs together without having to deal with the bottlenecks or configuration hassles normally associated with conventional routers.

Routing for unicast traffic is supported with the Routing Information Protocol (RIP) and the Open Shortest Path First (OSPF) protocol.

RIP – This protocol uses a distance-vector approach to routing. Routes are determined on the basis of minimizing the distance vector, or hop count, which serves as a rough estimate of transmission cost.

OSPF – This approach uses a link state routing protocol to generate a shortest-path tree, then builds up its routing table based on this tree. OSPF produces a more stable network because the participating routers act on network changes predictably and simultaneously, converging on the best route more quickly than RIP.

Address Resolution Protocol – The switch uses ARP and Proxy ARP to convert between IP addresses and MAC (i.e., hardware) addresses. This switch supports conventional ARP, which locates the MAC address corresponding to a given IP address. This allows the switch to use IP addresses for routing decisions and the corresponding MAC addresses to forward packets from one hop to the next. You can configure either static or dynamic entries in the ARP cache.

Proxy ARP allows hosts that do not support routing to determine the MAC address of a device on another network or subnet. When a host sends an ARP request for a remote network, the switch checks to see if it has the best route. If it does, it sends its own MAC address to the host. The host then sends traffic for the remote destination via the switch, which uses its own routing table to reach the destination on the other network.

Multicast Filtering – Specific multicast traffic can be assigned to its own VLAN to ensure that it does not interfere with normal network traffic and to guarantee real-time delivery by setting the required priority level for the designated VLAN. The switch uses IGMP Snooping and Query at Layer 2 and IGMP at Layer 3 to manage multicast group registration.

Multicast Routing – Routing for multicast packets is supported by the Distance Vector Multicast Routing Protocol (DVMRP) and Protocol-Independent Multicasting - Dense Mode (PIM-DM). These protocols work in conjunction with IGMP to filter and route multicast traffic. DVMRP is a more comprehensive implementation that maintains its own routing table, but is gradually being replaced by most network managers with PIM, Dense Mode and Sparse Mode. PIM is a very simple protocol that uses the routing table of the unicast routing protocol enabled on an interface. Dense Mode is designed for areas where the probability of multicast clients is relatively high, and the overhead of frequent flooding is justified. While Sparse mode is designed for network areas, such as the Wide Area Network, where the probability of multicast clients is low. This switch currently supports DVMRP and PIM-DM.

System Defaults

The switch's system defaults are provided in the configuration file "Factory_Default_Config.cfg." To reset the switch defaults, this file should be set as the startup configuration file (page 3-24).

The following table lists some of the basic system defaults.

Function	Parameter	Default
Console Port Connection	Baud Rate	9600
	Data bits	8
	Stop bits	1
	Parity	none
	Local Console Timeout	0 (disabled)

Function	Parameter	Default
Authentication	Privileged Exec Level	Username “admin” Password “admin”
	Normal Exec Level	Username “guest” Password “guest”
	Enable Privileged Exec from Normal Exec Level	Password “super”
	RADIUS Authentication	Disabled
	802.1x Port Authentication	Disabled
Web Management	HTTP Server	Enabled
	HTTP Port Number	80
SNMP	Community Strings	“public” (read only) “private” (read/write)
	Traps	Authentication traps: enabled Link-up-down events: enabled
Port Configuration	Admin Status	Enabled
	Auto-negotiation	Enabled
	Flow Control	Disabled
	Port Capability	100BASE-TX – 10 Mbps half duplex 10 Mbps full duplex 100 Mbps half duplex 100 Mbps full duplex Full-duplex flow control disabled 1000BASE-T – 10 Mbps half duplex 10 Mbps full duplex 100 Mbps half duplex 100 Mbps full duplex 1000 Mbps full duplex Full-duplex flow control disabled Symmetric flow control disabled

Function	Parameter	Default
	Port Capability	1000BASE-SX/LX/LH – 1000 Mbps full duplex Full-duplex flow control disabled Symmetric flow control disabled
Rate Limiting	Input and output limits	Disabled
Port Trunking	Static Trunks	None
	LACP (all ports)	Disabled
Broadcast Storm Protection	Status	Enabled (all ports)
	Broadcast Limit Rate	500 packets per second
Spanning Tree Protocol	Status	Enabled (Defaults: All values based on IEEE 802.1w)
	Fast Forwarding (Edge Port)	Disabled
Address Table	Aging Time	300 seconds
Virtual LANs	Default VLAN	1
	PVID	1
	Acceptable Frame Type	All
	Ingress Filtering	Disabled
	Switchport Mode (Egress Mode)	Hybrid: tagged/untagged frames
	GVRP (global)	Disabled
	GVRP (port interface)	Disabled
Traffic Prioritization	Ingress Port Priority	0
	Weighted Round Robin	Class 0: 1 Class 1: 4 Class 2: 16 Class 3: 64

Function	Parameter	Default
	IP Precedence Priority	Disabled
	IP DSCP Priority	Disabled
	IP Port Priority	Disabled
IP Settings	Management. VLAN	Any VLAN configured with an IP address
	IP Address	0.0.0.0
	Subnet Mask	255.0.0.0
	Default Gateway	0.0.0.0
	DHCP	Client: Disabled Relay: Disabled Server: Disabled
	BOOTP	Disabled
	ARP	Enabled Cache Timeout: 20 minutes Proxy: Disabled
Unicast Routing	RIP	Disabled
	OSPF	Disabled
Multicast Filtering	IGMP Snooping (Layer 2)	Snooping: Enabled Querier: Disabled
	IGMP (Layer 3)	Disabled
Multicast Routing	DVMRP	Disabled
	PIM-DM	Disabled
System Log	Status	Enabled
	Messages Logged	Levels 0-7 (all)
	Messages Logged to Flash	Levels 0-3

CHAPTER 2

INITIAL CONFIGURATION

Connecting to the Switch

Configuration Options

The switch includes a built-in network management agent. The agent offers a variety of management options, including SNMP, RMON and a Web-based interface. A PC may also be connected directly to the switch for configuration and monitoring via a command line interface (CLI).

Note: The IP address for this switch is unassigned by default. To change this address, see “Setting an IP Address” on page 2-6.

The switch’s HTTP Web agent allows you to configure switch parameters, monitor port connections, and display statistics using a standard Web browser such as Netscape Navigator version 6.2 and higher or Microsoft IE version 5.0 and higher. The switch’s Web management interface can be accessed from any computer attached to the network.

The CLI program can be accessed by a direct connection to the RS-232 serial console port on the switch, or remotely by a Telnet connection over the network.

The switch’s management agent also supports SNMP (Simple Network Management Protocol). This SNMP agent permits the switch to be managed from any system in the network using network management software such as HP OpenView.

The switch's Web interface, CLI configuration program, and SNMP agent allow you to perform the following management functions:

- Set user names and passwords for up to 16 users
- Set an IP interface for a management VLAN
- Configure SNMP parameters
- Enable/disable any port
- Set the speed/duplex mode for any port
- Configure the bandwidth of any port by limiting input or output rates
- Configure up to 255 IEEE 802.1Q VLANs
- Enable GVRP automatic VLAN registration
- Configure IP routing for unicast or multicast traffic
- Configure IGMP multicast filtering
- Upload and download system firmware via TFTP
- Upload and download switch configuration files via TFTP
- Configure Spanning Tree parameters
- Configure Class of Service (CoS) priority queuing
- Configure up to six static or LACP trunks
- Enable port mirroring
- Set broadcast storm control on any port
- Display system information and statistics

Required Connections

The switch provides an RS-232 serial port that enables a connection to a PC or terminal for monitoring and configuring the switch. A null-modem console cable is provided with the switch.

Attach a VT100-compatible terminal, or a PC running a terminal emulation program to the switch. You can use the console cable provided with this package, or use a null-modem cable that complies with the wiring assignments shown in the Installation Guide.

To connect a terminal to the console port, complete the following steps:

1. Connect the console cable to the serial port on a terminal, or a PC running terminal emulation software, and tighten the captive retaining screws on the DB-9 connector.
2. Connect the other end of the cable to the RS-232 serial port on the switch.
3. Make sure the terminal emulation software is set as follows:
 - Select the appropriate serial port (COM port 1 or COM port 2).
 - Set the data rate to 9600 baud.
 - Set the data format to 8 data bits, 1 stop bit, and no parity.
 - Set flow control to none.
 - Set the emulation mode to VT100.
 - When using HyperTerminal, select Terminal keys, not Windows keys.

- Notes:**
1. When using HyperTerminal with Microsoft® Windows® 2000, make sure that you have Windows 2000 Service Pack 2 or later installed. Windows 2000 Service Pack 2 fixes the problem of arrow keys not functioning in HyperTerminal's VT100 emulation. See www.microsoft.com for information on Windows 2000 service packs.
 2. Refer to "Line Commands" on page 4-13 for a complete description of console configuration options.
 3. Once you have set up the terminal correctly, the console login screen will be displayed.

For a description of how to use the CLI, see "Using the Command Line Interface" on page 4-1. For a list of all the CLI commands and detailed information on using the CLI, refer to "Command Groups" on page 4-11.

Remote Connections

Prior to accessing the switch's onboard agent via a network connection, you must first configure it with a valid IP address, subnet mask, and default gateway using a console connection, DHCP or BOOTP protocol.

The IP address for this switch is unassigned by default. To manually configure this address or enable dynamic address assignment via DHCP or BOOTP, see "Setting an IP Address" on page 2-6.

- Notes:**
1. This switch supports four concurrent Telnet sessions.
 2. Each VLAN group can be assigned its own IP interface address (page 2-6). You can manage the switch via any of these addresses.

After configuring the switch's IP parameters, you can access the onboard configuration program from anywhere within the attached network. The onboard configuration program can be accessed using Telnet from any computer attached to the network. The switch can also be managed by any computer using a Web browser (Internet Explorer 5.0 or above, or Netscape Navigator 6.2 or above), or from a network computer using SNMP network management software.

Note: The onboard program only provides access to basic configuration functions. To access the full range of SNMP management functions, you must use SNMP-based network management software.

Basic Configuration

Console Connection

The CLI program provides two different command levels — normal access level (Normal Exec) and privileged access level (Privileged Exec). The commands available at the Normal Exec level are a limited subset of those available at the Privileged Exec level and allow you to only display information and use basic utilities. To fully configure switch parameters, you must access the CLI at the Privileged Exec level.

Access to both CLI levels are controlled by user names and passwords. The switch has a default user name and password for each level. To log into the CLI at the Privileged Exec level using the default user name and password, perform these steps:

1. To initiate your console connection, press <Enter>. The “User Access Verification” procedure starts.
2. At the Username prompt, enter “admin.”
3. At the Password prompt, also enter “admin.” (The password characters are not displayed on the console screen.)
4. The session is opened and the CLI displays the “Console#” prompt indicating you have access at the Privileged Exec level.

Setting Passwords

Note: If this is your first time to log into the CLI program, you should define new passwords for both default user names using the “username” command, record them and put them in a safe place.

Passwords can consist of up to 8 alphanumeric characters and are case sensitive. To prevent unauthorized access to the switch, set the passwords as follows:

1. Open the console interface with the default user name and password “admin” to access the Privileged Exec level.
2. Type “configure” and press <Enter>.
3. Type “username guest password 0 *password*,” for the Normal Exec level, where *password* is your new password. Press <Enter>.
4. Type “username admin password 0 *password*,” for the Privileged Exec level, where *password* is your new password. Press <Enter>.

```
Username: admin
Password:
```

```
CLI session with the ES-3626G is opened.
To end the CLI session, enter [Exit].
```

```
Console#configure
Console(config)#username guest password 0 [password]
Console(config)#username admin password 0 [password]
Console(config)#
```

Setting an IP Address

You must establish IP address information for the switch to obtain management access through the network. This can be done in either of the following ways:

Manual — You have to input the information, including IP address and subnet mask. If your management station is not in the same IP subnet as the switch, you will also need to specify the default gateway router.

Dynamic — The switch sends IP configuration requests to BOOTP or DHCP address allocation servers on the network.

Manual Configuration

You can manually assign an IP address to the switch. You may also need to specify a default gateway that resides between this device and management stations that exist on another network segment (if routing is not enabled on this switch). Valid IP addresses consist of four decimal numbers, 0 to 255, separated by periods. Anything outside this format will not be accepted by the CLI program.

Note: The IP address for this switch is unassigned by default.

Before you can assign an IP address to the switch, you must obtain the following information from your network administrator:

- IP address for the switch
- Default gateway for the network
- Network mask for this network

To assign an IP address to the switch, complete the following steps:

1. From the Privileged Exec level global configuration mode prompt, type “interface vlan 1” to access the interface-configuration mode. Press <Enter>.
2. Type “ip address *ip-address netmask*,” where “ip-address” is the switch IP address and “netmask” is the network mask for the network. Press <Enter>.
3. Type “exit” to return to the global configuration mode prompt. Press <Enter>.
4. To set the IP address of the default gateway for the network to which the switch belongs, type “ip default-gateway *gateway*,” where “gateway” is the IP address of the default gateway. Press <Enter>.

```
Console(config)#interface vlan 1
Console(config-if)#ip address 192.168.1.5 255.255.255.0
Console(config-if)#exit
Console(config)#ip default-gateway 192.168.1.254
Console(config)#
```

Dynamic Configuration

If you select the “bootp” or “dhcp” option, IP will be enabled but will not function until a BOOTP or DHCP reply has been received. You therefore need to use the “ip dhcp restart client” command to start broadcasting service requests. Requests will be sent periodically in an effort to obtain IP configuration information. (BOOTP and DHCP values can include the IP address, subnet mask, and default gateway.)

If the “bootp” or “dhcp” option is saved to the startup-config file (step 6), then the switch will start broadcasting service requests as soon as it is powered on.

To automatically configure the switch by communicating with BOOTP or DHCP address allocation servers on the network, complete the following steps:

1. From the Global Configuration mode prompt, type “interface vlan 1” to access the interface-configuration mode. Press <Enter>.
2. At the interface-configuration mode prompt, use one of the following commands:
 - To obtain IP settings via DHCP, type “ip address dhcp” and press <Enter>.
 - To obtain IP settings via BOOTP, type “ip address bootp” and press <Enter>.
3. Type “end” to return to the Privileged Exec mode. Press <Enter>.
4. Type “ip dhcp restart client” to begin broadcasting service requests. Press <Enter>.
5. Wait a few minutes, and then check the IP configuration settings by typing the “show ip interface” command. Press <Enter>.

6. Then save your configuration changes by typing “copy running-config startup-config.” Enter the startup file name and press <Enter>.

```
Console(config)#interface vlan 1
Console(config-if)#ip address dhcp
Console(config-if)#end
Console#ip dhcp restart client
Console#show ip interface
Vlan 1 is up, addressing mode is DHCP
  Interface address is 10.1.0.54, mask is 255.255.255.0, Primary
  MTU is 1500 bytes
  Proxy ARP is disabled
  Split horizon is enabled
Console#copy running-config startup-config
Startup configuration file name []: startup
\Write to FLASH Programming.

\Write to FLASH finish.
Success.
```

Enabling SNMP Management Access

The switch can be configured to accept management commands from Simple Network Management Protocol (SNMP) applications such as HP OpenView. You can configure the switch to (1) respond to SNMP requests or (2) generate SNMP traps.

When SNMP management stations send requests to the switch (either to return information or to set a parameter), the switch provides the requested data or sets the specified parameter. The switch can also be configured to send information to SNMP managers (without being requested by the managers) through trap messages, which inform the manager that certain events have occurred.

Community Strings

Community strings are used to control management access to SNMP stations, as well as to authorize SNMP stations to receive trap messages from the switch. You therefore need to assign community strings to specified users or user groups, and set the access level.

The default strings are:

- **public** - with read-only access. Authorized management stations are only able to retrieve MIB objects.
- **private** - with read-write access. Authorized management stations are able to both retrieve and modify MIB objects.

Note: If you do not intend to utilize SNMP, we recommend that you delete both of the default community strings. If there are no community strings, then SNMP management access to the switch is disabled.

To prevent unauthorized access to the switch via SNMP, it is recommended that you change the default community strings.

To configure a community string, complete the following steps:

1. From the Privileged Exec level global configuration mode prompt, type “snmp-server community *string mode*,” where “string” is the community access string and “mode” is **rw** (read/write) or **ro** (read only). Press <Enter>. (Note that the default mode is read only.)
2. To remove an existing string, simply type “no snmp-server community *string*,” where “string” is the community access string to remove. Press <Enter>.

```
Console(config)#snmp-server community admin rw
Console(config)#snmp-server community private
Console(config)#
```

Trap Receivers

You can also specify SNMP stations that are to receive traps from the switch.

To configure a trap receiver, complete the following steps:

1. From the Privileged Exec level global configuration mode prompt, type “snmp-server host *host-address community-string*,” where “host-address” is the IP address for the trap receiver and “community-string” is the string associated with that host. Press <Enter>.
2. In order to configure the switch to send SNMP notifications, you must enter at least one snmp-server enable traps command. Type “snmp-server enable traps *type*,” where “type” is either **authentication** or **link-up-down**. Press <Enter>.

```
Console(config)#snmp-server enable traps link-up-down
Console(config)#
```

Saving Configuration Settings

Configuration commands only modify the running configuration file and are not saved when the switch is rebooted. To save all your configuration changes in nonvolatile storage, you must copy the running configuration file to the start-up configuration file using the “copy” command.

To save the current configuration settings, enter the following command:

1. From the Privileged Exec mode prompt, type “copy running-config startup-config” and press <Enter>.
2. Enter the name of the start-up file. Press <Enter>.

```
Console#copy running-config startup-config
Startup configuration file name []: startup
\Write to FLASH Programming.

\Write to FLASH finish.
Success.

Console#
```

Managing System Files

The switch's flash memory supports three types of system files that can be managed by the CLI program, Web interface, or SNMP. The switch's file system allows files to be uploaded and downloaded, copied, deleted, and set as a start-up file.

The three types of files are:

- **Configuration** — This file stores system configuration information and is created when configuration settings are saved. Saved configuration files can be selected as a system start-up file or can be uploaded via TFTP to a server for backup. A file named “Factory_Default_Config.cfg” contains all the system default settings and cannot be deleted from the system. See “Saving or Restoring Configuration Settings” on page 3-23 for more information.
- **Operation Code** — System software that is executed after boot-up, also known as run-time code. This code runs the switch operations and provides the CLI and Web management interfaces. See “Managing Firmware” on page 3-22 for more information.
- **Diagnostic Code** — Software that is run during system boot-up, also known as POST (Power On Self-Test). This code also provides a facility to upload firmware files to the system directly through the console port. See “Upgrading Firmware via the Serial Port” on page B-1.

Due to the size limit of the flash memory, the switch supports only two operation code files. However, you can have as many diagnostic code files and configuration files as available flash memory space allows.

In the system flash memory, one file of each type must be set as the start-up file. During a system boot, the diagnostic and operation code files set as the start-up file are run, and then the start-up configuration file is loaded.

Note that configuration files should be downloaded using a file name that reflects the contents or usage of the file settings. If you download directly to the running-config, the system will reboot, and the settings will have to be copied from the running-config to a permanent file.

INITIAL CONFIGURATION

CHAPTER 3

CONFIGURING THE SWITCH

Using the Web Interface

This switch provides an embedded HTTP Web agent. Using a Web browser you can configure the switch and view statistics to monitor network activity. The Web agent can be accessed by any computer on the network using a standard Web browser (Internet Explorer 5.0 or above, or Netscape Navigator 6.2 or above).

Note: You can also use the Command Line Interface (CLI) to manage the switch over a serial connection to the console port or via Telnet. For more information on using the CLI, refer to Chapter 4 “Command Line Interface.”

Prior to accessing the switch from a Web browser, be sure you have first performed the following tasks:

1. Configure the switch with a valid IP address, subnet mask, and default gateway using an out-of-band serial connection, BOOTP or DHCP protocol. (See “Setting the Switch’s IP Address” on page 3-17.)
2. Set user names and passwords using an out-of-band serial connection. Access to the Web agent is controlled by the same user names and passwords as the onboard configuration program. (See “Configuring the Logon Password” on page 3-28.)
3. After you enter a user name and password, you will have access to the system configuration program.

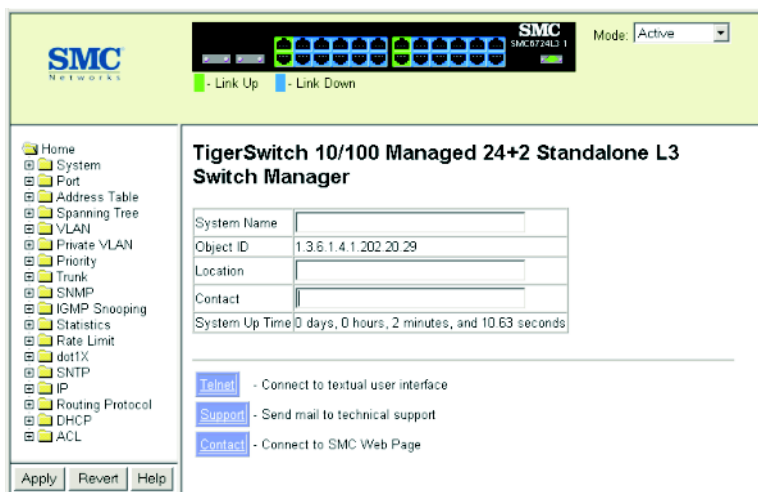
- Notes:**
1. You are allowed three attempts to enter the correct password; on the third failed attempt the current connection is terminated.
 2. If you log into the Web interface as guest (Normal Exec level), you can view the configuration settings or change the guest password. If you log in as “admin” (Privileged Exec level), you can change the settings on any page.
 3. If the path between your management station and this switch does not pass through any device that uses the Spanning Tree Algorithm, then you can set the switch port attached to your management station to fast forwarding (i.e., enable Admin Edge Port) to improve the switch’s response time to management commands issued through the Web interface. See “Configuring Interface Settings” on page 3-99.

Navigating the Web Browser Interface

To access the Web-browser interface you must first enter a user name and password. The administrator has Read/Write access to all configuration parameters and statistics. The default user name and password for the administrator is “admin.”

Home Page

When your Web browser connects with the switch’s Web agent, the home page is displayed as shown below. The home page displays the Main Menu on the left side of the screen and System Information on the right side. The Main Menu links are used to navigate to other menus, and display configuration parameters and statistics.



SMC Networks

Mode: Active

Link Up Link Down

TigerSwitch 10/100 Managed 24+2 Standalone L3 Switch Manager

System Name

Object ID 1.3.6.1.4.1.202.20.29

Location

Contact

System Up Time 0 days, 0 hours, 2 minutes, and 10.63 seconds

[Telnet](#) - Connect to textual user interface

[Support](#) - Send mail to technical support

[Contact](#) - Connect to SMC Web Page

Apply Revert Help

Configuration Options

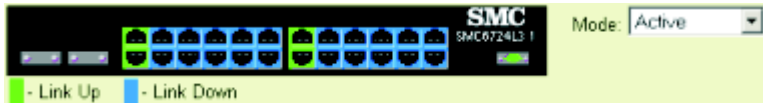
Configurable parameters have a dialog box or a drop-down list. Once a configuration change has been made on a page, be sure to click on the “Apply” or “Apply Changes” button to confirm the new setting. The following table summarizes the Web page configuration buttons.

Button	Action
Revert	Cancels specified values and restores current values prior to pressing “Apply” or “Apply Changes.”
Refresh	Immediately updates values for the current page.
Apply	Sets specified values to the system.
Apply Changes	Sets specified values to the system.

- Notes:**
1. To ensure proper screen refresh, be sure that Internet Explorer 5.x is configured as follows: Under the menu “Tools / Internet Options / General / Temporary Internet Files / Settings,” the setting for item “Check for newer versions of stored pages” should be “Every visit to the page.”
 2. When using Internet Explorer 5.0, you may have to manually refresh the screen after making configuration changes by pressing the browser’s refresh button.

Panel Display

The Web agent displays an image of the switch’s ports, indicating whether each link is up or down. The Mode can be set to display different information for the ports, including Active (i.e., up or down), Duplex (i.e., half or full duplex), or Flow Control (i.e., with or without flow control). Clicking on the image of a port opens the Port Configuration page as described on page 3-67.



Main Menu

Using the onboard Web agent, you can define system parameters, manage and control the switch, and all its ports, or monitor network conditions. The following table briefly describes the selections available from this program.

Menu	Description	Page
System		3-12
System Information	Provides basic system description, including contact information	3-12
Passwords	Assigns a new password for the current user	3-28
Radius	Configures RADIUS authentication parameters	3-30
Firmware	Manages code image files	3-22
Configuration	Manages switch configuration files	3-23
Reset	Restarts the switch	3-28
Bridge Extension	Shows the bridge extension parameters; enables GVRP VLAN registration protocol	3-16
Switch Information	Shows the number of ports, hardware/firmware version numbers, and power status	3-14
Port		3-63
Port Information	Displays port connection status	3-63
Trunk Information	Displays trunk connection status	3-63
Port Configuration	Configures port connection settings	3-67
Trunk Configuration	Configures trunk connection settings	3-67
Port Broadcast Control	Sets the broadcast storm threshold for each port	3-69
Mirror	Sets the source and target ports for mirroring	3-70
Address Table		3-84
Static Addresses	Displays entries for interface, address or VLAN	3-84
Dynamic Addresses	Displays or edits static entries in the Address Table	3-85
Address Aging	Sets timeout for dynamically learned entries	3-87

Menu	Description	Page
Spanning Tree		3-87
STA Information	Displays STA values used for the bridge	3-89
STA Configuration	Configures global bridge settings for STA	3-92
STA Port Information	Configures individual port settings for STA	3-95
STA Trunk Information	Configures individual trunk settings for STA	3-95
STA Port Configuration	Configures individual port settings for STA	3-99
STA Trunk Configuration	Configures individual trunk settings for STA	3-99
VLAN		3-102
VLAN Base Information	Displays information on the VLAN type supported by this switch	3-107
VLAN Current Table	Shows the current port members of each VLAN and whether or not the port is tagged or untagged	3-108
VLAN Static List	Used to create or remove VLAN groups	3-110
VLAN Static Table	Modifies the settings for an existing VLAN	3-111
VLAN Static Membership	Configures membership type for interfaces, including tagged, untagged or forbidden	3-113
VLAN Port Configuration	Specifies default PVID and VLAN attributes	3-114
VLAN Trunk Configuration	Specifies default trunk VID and VLAN attributes	3-114
Private VLAN		3-118
Private VLAN Status	Enables or disables the private VLAN	3-118
Private VLAN Link Configuration	Configures the private VLAN	3-119
Priority		3-120
Default Port Priority	Sets the default priority for each port	3-120
Default Trunk Priority	Sets the default priority for each trunk	3-120

Menu	Description	Page
Traffic Classes	Maps IEEE 802.1p priority tags to output queues	3-122
Queue Scheduling	Configures Weighted Round Robin queueing	3-124
IP Precedence/ DSCP Priority Status	Globally selects IP Precedence or DSCP Priority, or disables both.	3-126
IP Precedence Priority	Sets IP Type of Service priority, mapping the precedence tag to a class-of-service value	3-127
IP DSCP Priority	Sets IP Differentiated Services Code Point priority, mapping a DSCP tag to a class-of-service value	3-129
IP Port Status	Globally enables or disables IP Port Priority	3-131
IP Port Priority	Sets TCP/UDP port priority, defining the socket number and associated class-of-service value	3-131
Copy Settings	Copies port priority settings from source port to target port	3-131
Trunk		3-79
LACP Configuration	Allows ports to dynamically join trunks	3-80
Trunk Configuration	Specifies ports to group into static trunks	3-82
SNMP	Configures community strings and related trap functions	3-50
IGMP Snooping		3-134
IGMP Configuration	Enables multicast filtering; configures parameters for multicast query	3-137
Multicast Router Port Information	Displays the ports that are attached to a neighboring multicast router for each VLAN ID	3-139
Static Multicast Router Port Configuration	Assigns ports that are attached to a neighboring multicast router	3-140
IP Multicast Registration Table	Displays all multicast groups active on this switch, including multicast IP addresses and VLAN ID	3-142
IGMP Member Port Table	Indicates multicast addresses associated with the selected VLAN	3-143

Menu	Description	Page
Statistics	Lists Ethernet and RMON port statistics	3-71
Rate Limit		3-77
Input Rate Limit Port Configuration	Sets the input rate limit for each port	3-77
Input Rate Limit Trunk Configuration	Sets the input rate limit for each trunk	3-77
Output Rate Limit Port Configuration	Sets the output rate limit for each port	3-77
Output Rate Limit Trunk Configuration	Sets the output rate limit for each trunk	3-77
dot1X (IEEE 802.1x)	Port authentication	3-32
dot1X Information	Displays global configuration settings	3-34
dot1X Configuration	Configures protocol parameters	3-36
dot1X Port Configuration	Sets the authentication mode for individual ports	3-38
dot1X Statistics	Displays protocol statistics for the selected port	3-39
SNTP		3-25
SNTP Configuration	Configures SNTP client settings, including broadcast mode or a specified list of servers	3-26
Clock Time Zone	Sets the local time zone for the clock	3-27
IP		3-149
General		3-154
Global Settings	Enables or disables routing, specifies the default gateway	3-154
Routing Interface	Configures the IP interface for the specified VLAN	3-155
ARP		3-157
General	Sets the protocol timeout, and enables or disables proxy ARP for the specified VLAN	3-159
Static Addresses	Statically maps a physical address to an IP address	3-160

Menu	Description	Page
Dynamic Addresses	Shows dynamically learned entries in the IP routing table	3-161
Other Addresses	Shows internal addresses used by the switch	3-163
Statistics	Shows statistics on ARP requests sent and received	3-164
IGMP		3-144
Interface Settings	Configures Layer 3 IGMP for specific VLAN interfaces	3-145
Group Membership	Displays the current multicast groups learned via IGMP	3-148
Statistics		3-165
IP	Shows statistics for IP traffic, including the amount of traffic, address errors, routing, fragmentation and reassembly	3-165
ICMP	Shows statistics for ICMP traffic, including the amount of traffic, protocol errors, and the number of echoes, timestamps, and address masks	3-168
UDP	Shows statistics for UDP, including the amount of traffic and errors	3-170
TCP	Shows statistics for TCP, including the amount of traffic and TCP connection activity	3-171
Routing		3-151
Static Routes	Shows all static routing entries	3-172
Routing Table	Shows all routing entries, including local, static and dynamic routes	3-173
Multicast Routing		3-218
General Settings	Globally enables multicast routing	3-219
Multicast Routing Table	Shows each multicast route this switch has learned	3-219

Menu	Description	Page
Routing Protocol		3-152
RIP		3-175
General Settings	Enables or disables RIP, sets the global RIP version and timer values	3-176
Network Addresses	Configures the network interfaces that will use RIP	3-178
Interface Settings	Configure RIP parameters for each interface, including send and receive versions, message loopback prevention, and authentication	3-179
Statistics	Displays general information on update time, route changes and number of queries, as well as a list of statistics for known interfaces and neighbors	3-183
OSPF		3-186
General Configuration	Enables or disables OSPF; also configures the Router ID and various other global settings	3-188
Area Configuration	Specifies rules for importing routes into each area	3-192
Area Range Configuration	Configures route summaries to advertise at an area boundary	3-196
Interface Configuration	Shows area ID and designated router; also configures OSPF protocol settings and authentication for each interface	3-198
Virtual Link Configuration	Configures virtual link through transit area to backbone	3-204
Network Area Address Configuration	Defines OSPF areas and associated interfaces	3-206
Summary Address Configuration	Aggregates routes learned from other protocols for advertising into other autonomous systems	3-208
Redistribute Configuration	Redistributes routes from one routing domain to another	3-210

Menu	Description	Page
NSSA Settings	Configures settings for importing routes into or exporting routes out of not-so-stubby areas	3-212
Link State Database Information	Shows information about different OSPF Link State Advertisements (LSAs) stored in this router's database	3-213
Border Router Information	Displays routing table entries for area border routers and autonomous system boundary routers	3-216
Neighbor Information	Display information about neighboring routers on each interface within an OSPF area	3-217
DVMRP		3-222
General Settings	Configure global settings for prune and graft messages, and the exchange of routing information	3-223
Interface Settings	Enables/disables DVMRP per interface and sets route metric	3-227
Neighbor Information	Displays neighboring DVMRP routers	3-229
Routing Table	Displays DVMRP routing information	3-230
PIM-DM		
General Settings	Enables or disables PIM-DM globally for the switch	3-232
Interface Settings	Enables/disables PIM-DM per interface, configures protocol settings for hello, prune and graft messages	3-233
Interface Information	Displays summary information for each interface	3-236
Neighbor Information	Displays neighboring PIM-DM routers	3-237
DHCP		3-53
Relay Configuration	Specifies DHCP relay servers; enables or disables relay service	3-53
Server	Configures DHCP server parameters	3-53

Menu	Description	Page
General	Enables DHCP server; configures excluded address range	3-56
Pool Configuration	Configures address pools for network groups or a specific host	3-57
IP Binding	Displays addresses currently bound to DHCP clients	3-62
ACL		3-41
ACL Configuration	Configures packet filtering based on IP or MAC addresses	3-41
ACL Port Binding	Binds a port to the specified ACL	3-49

Basic Configuration

Displaying System Information

You can easily identify the system by displaying the device name, location and contact information.

Field Attributes

- **System Name** – Name assigned to the switch system.
- **Object ID** – MIB II object ID for switch's network management subsystem.
- **Location** – Specifies the system location.
- **Contact** – Administrator responsible for the system.
- **System Up Time** – Length of time the management agent has been up.

These additional parameters are displayed for the CLI.

- **MAC Address**^{*} – The physical layer address for this switch.
- **Web server** – Shows if management access via HTTP is enabled.
- **Web server port** – Shows TCP port number used by the Web interface.
- **POST result** – Shows results of the power-on self-test

* Web: See "Setting the IP Address" on page 3-9.

Web – Click System, System Information. Specify the system name, location, and contact information for the system administrator, then click Apply. (This page also includes a Telnet button that allows access to the Command Line Interface via Telnet.)

TigerSwitch 10/100 Managed 24+2 Standalone L3 Switch Manager

System Name	<input type="text"/>
Object ID	1.3.6.1.4.1.202.20.29
Location	<input type="text"/>
Contact	<input type="text"/>
System Up Time	0 days, 0 hours, 2 minutes, and 10.63 seconds

[Telnet](#) - Connect to textual user interface
[Support](#) - Send mail to technical support
[Contact](#) - Connect to SMC Web Page

CLI – Specify the hostname, location and contact information.

```

Console(config)#hostname R&D 5                                4-32
Console(config)#snmp-server location WC 9                     4-92
Console(config)#snmp-server contact Ted                       4-91
Console(config)#exit
Console#show system                                           4-51
System description: TigerSwitch 10/100 Managed 24+2 L3 Switch
System OID string: 1.3.6.1.4.1.202.20.29
System information
  System Up time: 0 days, 2 hours, 4 minutes, and 7.13 seconds
  System Name      : R&D 5
  System Location  : WC 9
  System Contact   : Ted
  MAC address      : 00-30-f1-47-58-3a
  Web server       : enable
  Web server port  : 80
  Ingress rate limit : Disabled
  POST result      :
Console#
  
```

Displaying Switch Hardware/Software Versions

Use the Switch Information page to display hardware/firmware version numbers for the main board and management software, as well as the power status of the system.

Field Attributes

Main Board

- **Serial Number** – The serial number of the switch.
- **Service Tag*** – Not implemented.
- **Number of Ports** – Number of built-in RJ-45 ports and expansion ports.
- **Hardware Version** – Hardware version of the main board.
- **Internal Power Status** – Displays the status of the internal power supply.
- **Redundant Power Status*** – Displays the status of the redundant power supply.

Management Software

- **Loader Version** – Version number of loader code.
- **Boot-ROM Version** – Version number of Power-On Self-Test (POST) and boot code.
- **Operation Code Version** – Version number of runtime code.
- **Role** – Shows that this switch is operating as Master (i.e., operating stand-alone).

Expansion Slots

- **Expansion Slot** – Indicates any installed module type.

* CLI only.

Web – Click System, Switch Information.

Switch Information	
Main Board:	
Serial Number	1111111111
Number of Ports	26
Hardware Version	R0A
Internal Power Status	Active
Management Software:	
Loader Version	0.0.6.5
Boot-ROM Version	0.0.5.2
Operation Code Version	1.2.0.4
Role	Master
Expansion Slot:	
Expansion Slot 1	1000Base-SX-SC MMF
Expansion Slot 2	1000BaseT

CLI – Use the following command to display version information.

```

Console#show version
Unit1
  Serial number      :1111111111
  Service tag        :
  Hardware version    :R0A
  Number of ports     :26
  Main power status   :up
  Redundant power status :not present
Agent(master)
  Unit id            :1
  Loader version      :0.0.6.5
  Boot rom version    :0.0.5.2
  Operation code version :0.0.2.24
Console#

```

4-52

Displaying Bridge Extension Capabilities

The Bridge MIB includes extensions for managed devices that support Multicast Filtering, Traffic Classes, and Virtual LANs. You can access these extensions to display default settings for the key variables, or to configure the global setting for GARP VLAN Registration Protocol (GVRP).

Command Attributes

- **Extended Multicast Filtering Services** – This switch does not support the filtering of individual multicast addresses based on GMRP (GARP Multicast Registration Protocol).
- **Traffic Classes** – This switch provides mapping of user priorities to multiple traffic classes. (Refer to “Class of Service Configuration” on page 3-120.)
- **Static Entry Individual Port** – This switch allows static filtering for unicast and multicast addresses. (Refer to “Setting Static Addresses” on page 3-84.)
- **VLAN Learning** – This switch uses Independent VLAN Learning (IVL), where each port maintains its own filtering database.
- **Configurable PVID Tagging** – This switch allows you to override the default Port VLAN ID (PVID used in frame tags) and egress status (VLAN-Tagged or Untagged) on each port. (Refer to “VLAN Configuration” on page 3-102.)
- **Local VLAN Capable** – This switch does not support multiple local bridges (i.e., multiple Spanning Trees).
- **GMRP** – GARP Multicast Registration Protocol (GMRP) allows network devices to register endstations with multicast groups. This switch does not support GMRP; it uses the Internet Group Management Protocol (IGMP) to provide automatic multicast filtering.
- **GVRP** – GARP VLAN Registration Protocol (GVRP) defines a way for switches to exchange VLAN information in order to register necessary VLAN members on ports across the network. This function should be enabled to permit VLANs groups which extend beyond the local switch. (Default: Disabled)

Web – Click System, Bridge Extension.

Bridge Capability

Extended Multicast Filtering Services	No
Traffic Classes	Enabled
Static Entry Individual Port	Yes
VLAN Learning	IVL
Configurable PVID Tagging	Yes
Local VLAN Capable	No

Traffic Classes	<input checked="" type="checkbox"/> Enable
GMRP	<input type="checkbox"/> Enable
GVRP	<input type="checkbox"/> Enable

CLI – Enter the following command.

```

Console#show bridge-ext
Max support vlan numbers: 255
Max support vlan ID: 4094
Extended multicast filtering services: No
Static entry individual port: Yes
VLAN learning: IVL
Configurable PVID tagging: Yes
Local VLAN capable: No
Traffic classes: Enabled
Global GVRP status: Disabled
GMRP: Disabled
Console#

```

4-176

Setting the Switch's IP Address

This section describes how to configure an initial IP interface for management access over the network. The IP address for this switch is unassigned by default. To manually configure an address, you need to change the switch's default settings (IP address 0.0.0.0 and netmask 255.0.0.0) to values that are compatible with your network. You may also need to establish a default gateway between the switch and management stations that exist on another network segment (if routing is not enabled on this switch).

You can manually configure a specific IP address, or direct the device to obtain an address from a BOOTP or DHCP server. Valid IP addresses consist of four decimal numbers, 0 to 255, separated by periods. Anything outside this format will not be accepted by the CLI program.

Command Usage

- This section describes how to configure a single local interface for initial access to the switch. To configure multiple IP interfaces on this switch, you must set up an IP interface for each VLAN (page 3-155).
- To enable routing between the different interfaces on this switch, you must enable IP routing (page 3-154).
- To enable routing between the interfaces defined on this switch and external network interfaces, you must configure static routes (page 3-172) or use dynamic routing; i.e., either RIP (page 3-175) or OSPF (page 3-186).
- The precedence for configuring IP interfaces is the IP / General / Routing Interface menu (page 3-155), static routes (page 3-172), and then dynamic routing.

Command Attributes

- **VLAN** – ID of the configured VLAN (1-4094, no leading zeroes). By default, all ports on the switch are members of VLAN 1. However, the management station can be attached to a port belonging to any VLAN, as long as that VLAN has been assigned an IP address.
- **IP Address Mode** – Specifies whether IP functionality is enabled via manual configuration (Static), Dynamic Host Configuration Protocol (DHCP), or Boot Protocol (BOOTP). If DHCP/BOOTP is enabled, IP will not function until a reply has been received from the server. Requests will be broadcast periodically by the switch for an IP address. (DHCP/BOOTP values can include the IP address, subnet mask, and default gateway.)
- **IP Address** – Address of the VLAN interface through which the management station is attached. Valid IP addresses consist of four numbers, 0 to 255, separated by periods. (Default: 0.0.0.0)

- **Subnet Mask** – This mask identifies the host address bits used for routing to specific subnets. (Default: 255.0.0.0)
- **Default Gateway** – IP address of the gateway router between this device and management stations that exist on other network segments. (Default: 0.0.0.0)

Manual Configuration

Web – Click IP, General, Routing Interface. Select the VLAN to which the management station is attached, set the IP Address Mode to “Static” and specify a “Primary” interface, enter the IP address and subnet mask, then click Set IP Configuration.

Routing Interface	
VLAN	1
IP Address Mode	Static Primary
IP Address	10.1.0.253
Subnet Mask	255.255.255.0
<input type="button" value="Set IP Configuration"/> <input type="button" value="Remove IP Address"/>	

Click IP, Global Setting. If this switch and management stations exist on other network segments, then specify the default gateway, and click Apply.

Global Settings	
IP Routing Status	Enabled
Default Gateway	10.1.0.254
<input type="button" value="Clear default gateway"/>	

CLI – Specify the management interface, IP address and default gateway.

```
Console#config
Console(config)#interface vlan 1 4-119
Console(config-if)#ip address 10.1.0.254 255.255.255.0 4-216
Console(config-if)#exit
Console(config)#ip default-gateway 192.168.1.254 4-218
Console(config)#
```

Using DHCP/BOOTP

If your network provides DHCP/BOOTP services, you can configure the switch to be dynamically configured by these services.

Web – Click IP, General, Routing Interface. Specify the VLAN to which the management station is attached, set the IP Address Mode to DHCP or BOOTP. Click Apply to save your changes. Then click Restart DHCP to immediately request a new address. Note that the switch will also broadcast a request for IP configuration settings on each power reset.

Routing Interface

VLAN	1	
IP Address Mode	DHCP	Primary
IP Address	10.1.0.253	
Subnet Mask	255.255.255.0	

Set IP ConfigurationRemove IP Address

Restart DHCP

Note: If you lose your management connection, use a console connection and enter “show ip interface” to determine the new switch address.

CLI – Specify the management interface, and set the IP Address Mode to DHCP or BOOTP, and then enter the “ip dhcp restart client” command.

```
Console#config
Console(config)#interface vlan 1
Console(config-if)#ip address dhcp
Console(config-if)#end
Console#ip dhcp restart client
Console#show ip interface
Vlan 1 is up, addressing mode is Dhcp
  Interface address is 10.1.0.253, mask is 255.255.255.0, Primary
  MTU is 1500 bytes
  Proxy ARP is disabled
  Split horizon is enabled
Console#
```

Renewing DHCP – DHCP may lease addresses to clients indefinitely or for a specific period of time. If the address expires or the switch is moved to another network segment, you will lose management access to the switch. In this case, you can reboot the switch or submit a client request to restart DHCP service via the CLI.

Web – If the address assigned by DHCP is no longer functioning, you will not be able to renew the IP settings via the Web interface. You can only restart DHCP service via the Web interface if the current address is still available.

CLI – Enter the following command to restart DHCP service.

```
Console#ip dhcp restart client
```

Managing Firmware

You can upload/download firmware to or from a TFTP server. By saving runtime code to a file on a TFTP server, that file can later be downloaded to the switch to restore operation. You can also set the switch to use new firmware without overwriting the previous version.

Command Attributes

- **TFTP Server IP Address** – The IP address of a TFTP server.
- **File Name** – The file name should not contain slashes (\ or /), the leading letter of the file name should not be a period (.), and the maximum length for file names on the TFTP server is 127 characters or 31 characters for files on the switch. (Valid characters: A-Z, a-z, 0-9, “.”, “-”, “_”)

Note: Up to two copies of the system software (i.e., the runtime firmware) can be stored in the file directory on the switch. The currently designated startup version of this file cannot be deleted.

Downloading System Software from a Server

When downloading runtime code, you can specify the destination file name to replace the current image, or first download the file using a different name from the current runtime code file, and then set the new file as the startup file.

Web – Click System, Firmware. Enter the IP address of the TFTP server, enter the file name of the software to download, select a file on the switch to overwrite or specify a new file name, then click Transfer from Server. To start the new firmware, reboot the system via the System/Reset menu.

The screenshot shows a web interface titled "Transfer Operation Code Image File from Server". It contains a form with the following fields:

Current Operation Code Version	1.2.0.4		
TFTP Server IP Address	<input type="text" value="192.168.1.19"/>		
Source File Name	<input type="text" value="V12.bix"/>		
Destination File Name	<input type="text" value="V1204-17"/>	<input type="text" value="V1.2"/>	<input type="text"/>

Below the form is a button labeled "Transfer from Server".

If you download to a new destination file, then select the file from the drop-down box for the operation code used at startup, and click Apply Changes. To start the new firmware, reboot the system via the System/Reset menu.



Start-Up Operation Code Image File

File Name: V1.0

Apply Changes

CLI – Enter the IP address of the TFTP server, select “config” or “opcode” file type, then enter the source and destination file names, set the new file to start up the system, and then restart the switch.

Console#copy tftp file	4-53
TFTP server ip address: 10.1.0.19	
Choose file type:	
1. config: 2. opcode: <1-2>: 2	
Source file name: M100000.bix	
Destination file name: V1.0	
\Write to FLASH Programming.	
-Write to FLASH finish.	
Success.	
Console#config	
Console(config)#boot system opcode:V1.0	4-59
Console(config)#exit	
Console#reload	4-28

Saving or Restoring Configuration Settings

You can upload/download configuration settings to/from a TFTP server. The configuration file can be later downloaded to restore the switch’s settings.

Command Attributes

- **TFTP Server IP Address** – The IP address of a TFTP server.
- **File Name** — The configuration file name should not contain slashes (\ or /), the leading letter of the file name should not be a period (.), and the maximum length for file names on the TFTP server is 127 characters or

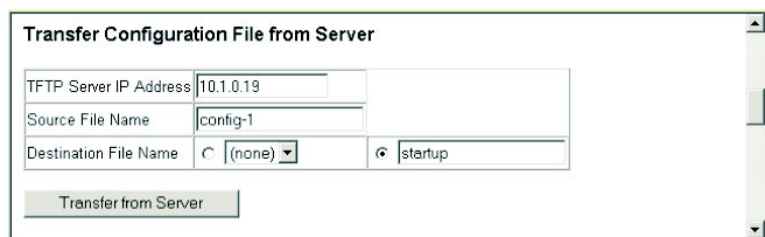
31 characters for files on the switch. (Valid characters: A-Z, a-z, 0-9, “.”, “-”, “_”)

Note: The maximum number of user-defined configuration files is limited only by available flash memory space.

Downloading Configuration Settings from a Server

You can download the configuration file under a new file name and then set it as the startup file, or you can specify the current startup configuration file as the destination file to directly replace it. Note that the file “Factory_Default_Config.cfg” can be copied to the TFTP server, but cannot be used as the destination on the switch.

Web – Click System, Configuration. Enter the IP address of the TFTP server, enter the name of the file to download, select a file on the switch to overwrite or specify a new file name, and then click Transfer from Server.



The screenshot shows a web interface titled "Transfer Configuration File from Server". It contains three input fields: "TFTP Server IP Address" with the value "10.1.0.19", "Source File Name" with the value "config-1", and "Destination File Name" which has a dropdown menu currently showing "(none)". To the right of the dropdown is a text input field containing "startup". Below these fields is a button labeled "Transfer from Server".

If you download to a new file name, then select the new file from the drop-down box for Startup Configuration File, and press Apply Changes. To use the new settings, reboot the system via the System/Reset menu.



The screenshot shows a web interface titled "Start-Up Configuration File". It contains a dropdown menu labeled "File Name" which currently shows "startup". Below the dropdown is a button labeled "Apply Changes".

CLI – Enter the IP address of the TFTP server, specify the source file on the server, set the startup file name on the switch, and then restart the switch.

```
Console#copy tftp startup-config                                4-53
TFTP server ip address: 192.168.1.19
Source configuration file name: config-1
Startup configuration file name [] : startup
\Write to FLASH Programming.
-Write to FLASH finish.
Success.
Console#reload
```

If you download the startup configuration file under a new file name, you can set this file as the startup file at a later time, and then restart the switch.

```
Console#config
Console(config)#boot system config: startup-new                4-59
Console(config)#exit
Console#reload                                                  4-28
```

Setting the System Clock

Simple Network Time Protocol (SNTP) allows the switch to set its internal clock based on periodic updates from a time server (SNTP or NTP).

Maintaining an accurate time on the switch enables the system log to record meaningful dates and times for event entries. Without SNTP, the switch will only record the time from the factory default set at the last bootup.

This switch acts as an SNTP client in two modes:

Unicast – The switch periodically sends a request for a time update to a configured time server. You can configure up to three time server IP addresses. The switch will attempt to poll each server in the configured sequence.

Broadcast – The switch sets its clock from a time server in the same subnet that broadcasts time updates. If there is more than one SNTP server, the switch accepts the first broadcast it detects and ignores broadcasts from other servers.

Configuring SNTP

You can configure the switch to send time synchronization requests to specific time servers (i.e., client mode), update its clock based on broadcasts from time servers, or use both methods. When both methods are enabled, the switch will update its clock using information broadcast from time servers, but will query the specified server(s) if a broadcast is not received within the polling interval.

Command Attributes

- **Current Time** – Displays the current time.
- **SNTP Client** – Configures the switch to operate as an SNTP unicast client. This mode requires at least one time server to be specified in the SNTP Server field.
- **SNTP Broadcast client** – Configures the switch to operate as an SNTP broadcast client. This mode requires no other configuration settings; the switch will obtain time updates from time server broadcasts (using the multicast address 224.0.1.1).
- **SNTP Poll Interval** – Sets the interval between sending requests for a time update from a time server when set to SNTP Client mode. (Range: 16-16284 seconds; Default: 16 seconds)
- **SNTP Server** – In unicast mode, sets the IP address for up to three time servers. The switch attempts to update the time from the first server. If this fails it attempts an update from the next server in the sequence.

Web – Select SNTP, SNTP Configuration. Modify any of the required parameters, and click Apply.

SNTP Configuration			
Current Time	Jan 8 15:30:37 2001		
SNTP Client	<input checked="" type="checkbox"/> Enable		
SNTP Broadcast client	<input checked="" type="checkbox"/> Enable		
SNTP Poll Interval (16-16384)	16		
SNTP Server	10.1.0.19	137.82.140.80	128.250.36.2

CLI – This example configures the switch to operate as an SNTP broadcast client.

Console(config)#sntp client	4-42
Console(config)#sntp poll 16	4-44
Console(config)#sntp server 10.1.0.19 137.82.140.80	
128.250.36.2	4-43
Console(config)#sntp broadcast client	4-45
Console(config)#	

Setting the Time Zone

SNTP uses Coordinated Universal Time (or UTC, formerly Greenwich Mean Time, or GMT) based on the time at the Earth's prime meridian, zero degrees longitude. To display a time corresponding to your local time, you must indicate the number of hours and minutes your time zone is east (before) or west (after) of UTC.

Command Attributes

- **Name** – Assigns a name to the time zone.
- **Hours (0-12)** – The number of hours before/after UTC.
- **Minutes (0-59)** – The number of minutes before/after UTC.
- **Direction** – Configures the time zone to be before (east) or after (west) UTC.

Web – Select SNTP, Clock Time Zone. Set the offset for your time zone relative to the UTC, and click Apply.

Clock Time Zone

Name	Taiwan
Hours(0~13)	8
Minutes(0~59)	0
Direction	<input type="radio"/> before-utc <input checked="" type="radio"/> after-utc

CLI - This example shows how to set the time zone for the system clock.

Console(config)#clock timezone 06.00 hours 6 minute 58	
before-UTC	4-46
Console#	

Resetting the System

Web – Click System, Reset. Click the Reset button to restart the switch.



CLI – Use the reload command to restart the switch.

```
Console#reload  
System will be restarted, continue <y/n>?
```

4-28

Note: When restarting the system, it will always run the Power-On Self-Test.

User Authentication

Use the Passwords or Radius menu to restrict management access based on specified user names and passwords. You can manually configure access rights on the switch (Passwords menu), or you can use a remote access authentication server based on the RADIUS protocol (Radius menu). After you set up user names and passwords on the RADIUS server, you can use IEEE 802.1x port authentication to control access to specific ports (dot1X menu).

Configuring the Logon Password

The guest only has read access for most configuration parameters. However, the administrator has write access for all parameters governing the onboard agent. You should therefore assign a new administrator password as soon as possible, and store it in a safe place. (If for some reason your password is lost, you can delete all the user-defined configuration files to restore the factory defaults and the default password as described in “Upgrading Firmware via the Serial Port” on page B-1.)

The default guest name is “guest” with the password “guest.” The default administrator name is “admin” with the password “admin.” Note that user names can only be assigned via the CLI.

Command Attributes

- **User Name*** – The name of the user.
(Maximum length: 8 characters; maximum number of users: 5)
- **Access Level*** – Specifies the user level.
(Options: Normal and Privileged)
- **Password** – Specifies the user password.
(Range: 0-8 characters plain text, case sensitive)

* CLI only.

Web – Click System, Passwords. To change the password for the current user, enter the old password, enter the new password, confirm it by entering it again, then click Apply.

Passwords

Old Password	<input type="password"/>
New Password	<input type="password"/>
Confirm Password	<input type="password"/>

CLI – Assign a user name to access-level 15 (i.e., administrator), then specify the password.

```

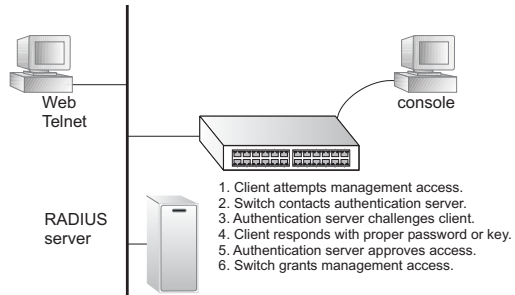
Console(config)#username bob access-level 15
Console(config)#username bob password 0 smith
Console(config)#
  
```

4-33

Configuring Local/Remote Logon Authentication

Use the Authentication Settings menu to restrict management access based on specified user names and passwords. You can manually configure access rights on the switch, or you can use a remote access authentication server based on the RADIUS protocol.

Remote Authentication Dial-in User Service (RADIUS) is a logon authentication protocol that uses software running on a central server to control access to RADIUS-compliant devices on the network.



An authentication server contains a database of multiple user name/password pairs with associated privilege levels for each user that requires management access to the switch.

Command Usage

- By default, management access is always checked against the authentication database stored on the local switch. If a remote authentication server is used, you must specify the authentication sequence and the corresponding parameters for the remote authentication protocol. Local and remote logon authentication control management access via the console port, web browser, or Telnet.
- RADIUS uses UDP, which only offers best effort delivery. Also, RADIUS encrypts only the password in the access-request packet from the client to the server.
- RADIUS logon authentication assigns a specific privilege level for each user name/password pair. The user name, password, and privilege level must be configured on the authentication server.
- You can specify one to two authentication methods for any user to indicate the authentication sequence. For example, if you select

(1) RADIUS and (2) Local, the user name and password on the RADIUS server is verified first. If the RADIUS server is not available, then the local user name and password is checked.

Command Attributes

- **Authentication** – Select the authentication, or authentication sequence required:
 - Local – User authentication is performed only locally by the switch.
 - Radius – User authentication is performed using a RADIUS server only.
 - Radius, Local – User authentication is attempted first using a RADIUS server, then locally by the switch.
 - Local, Radius – User authentication is first attempted locally by the switch, then using a RADIUS server.
- **Server IP Address** – Address of authentication server.
(Default: 10.1.0.1)
- **Server Port Number** – Network (UDP) port of authentication server used for authentication messages. (Range: 1-65535; Default: 1812)
- **Secret Text String** – Encryption key used to authenticate logon access for client. Do not use blank spaces in the string. (Maximum length: 20 characters)
- **Number of Server Transmits** – Number of times the switch will try to authenticate logon access via the authentication server. (Range: 1-30; Default: 2)
- **Timeout for a reply** – The number of seconds the switch waits for a reply from the RADIUS server before it resends the request. (Range: 1-65535; Default: 5)

Note: The local switch user database has to be set up by manually entering user names and passwords using the CLI. (See “username” on page 33.)

Web – Click System, Radius. To configure local or remote authentication preferences, specify the authentication sequence (i.e., one to two methods), fill in the parameters for RADIUS authentication if selected, and click Apply.

Radius Settings	
Authentication	Local ▾
Server IP Address	192.168.1.25
Server Port Number	1812
Secret Text String	green
Number of Server Transmits	5
Timeout for a reply (sec)	10

CLI – Specify all the required parameters to enable logon authentication.

```
Console(config)#authentication login radius 4-60
Console(config)#radius-server host 192.168.1.25 4-62
Console(config)#radius-server port 181 4-63
Console(config)#radius-server key green 4-63
Console(config)#radius-server retransmit 5 4-64
Console(config)#radius-server timeout 10 4-65
Console#show radius-server 4-65
Server IP address: 192.168.1.25
Communication key with radius server:
Server port number: 181
Retransmit times: 5
Request timeout: 10
Console(config)#
```

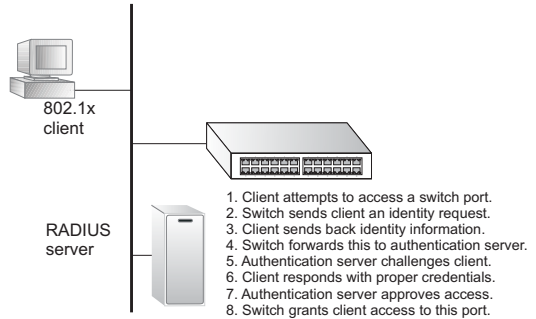
Configuring 802.1x Port Authentication

Network switches can provide open and easy access to network resources by simply attaching a client PC. Although this automatic configuration and access is a desirable feature, it also allows unauthorized personnel to easily intrude and possibly gain access to sensitive network data.

The IEEE 802.1x (dot1x) standard defines a port-based access control procedure that prevents unauthorized access to a network by requiring users to first submit credentials for authentication. Access to all switch

ports in a network can be centrally controlled from a server, which means that authorized users can use the same credentials for authentication from any point within the network.

This switch uses the Extensible Authentication Protocol over LANs (EAPOL) to exchange authentication protocol messages with the client, and a remote RADIUS authentication server



to verify user identity and access rights. When a client (i.e., Supplicant) connects to a switch port, the switch (i.e., Authenticator) responds with an EAPOL identity request. The client provides its identity (such as a user name) in an EAPOL response to the switch, which it forwards to the RADIUS server. The RADIUS server verifies the client identity and sends an access challenge back to the client. The EAP packet from the RADIUS server contains not only the challenge, but the authentication method to be used. The client can reject the authentication method and request another, depending on the configuration of the client software and the RADIUS server. The authentication method can be MD5, TLS (Transport Layer Security), TTLS (Tunneled Transport Layer Security), or other. The client responds to the appropriate method with its credentials, such as a password or certificate. The RADIUS server verifies the client credentials and responds with an accept or reject packet. If authentication is successful, the switch allows the client to access the network. Otherwise, network access is denied and the port remains blocked.

The operation of dot1x on the switch requires the following:

- The switch must have an IP address assigned.
- RADIUS authentication must be enabled on the switch and the IP address of the RADIUS server specified.

- Each switch port that will be used must be set to dot1x “Auto” mode.
- Each client that needs to be authenticated must have dot1x client software installed and properly configured.
- The RADIUS server and 802.1x client support EAP. (The switch only supports EAPOL in order to pass the EAP packets from the server to the client.)
- The RADIUS server and client also have to support the same EAP authentication type – MD5, TLS, TTLS, PEAP, etc. (Some clients have native support in Windows, otherwise the dot1x client must support it.)

Displaying 802.1x Global Settings

The dot1x protocol includes global parameters that control the client authentication process that runs between the client and the switch (i.e., authenticator), as well as the client identity lookup process that runs between the switch and authentication server. These parameters are described in this section.

Command Attributes

- **dot1x Re-authentication** – Indicates if switch port requires a client to be re-authenticated after a certain period of time.
- **dot1x Max Request Count** – The maximum number of times the switch port will retransmit an EAP request packet to the client before it times out the authentication session.
- **Timeout for Quiet Period** – Indicates the time that a switch port waits after the Max Request Count has been exceeded before attempting to acquire a new client.
- **Timeout for Re-authentication Period** – Indicates the time period after which a connected client must be re-authenticated.
- **Timeout for TX Period** – The time period during an authentication session that the switch waits before re-transmitting an EAP packet.
- **Supplicant timeout** – The time the switch waits for a client response to an EAP request.

- **Server timeout** – The time the switch waits for a response from the authentication server (RADIUS) to an authentication request.
- **Re-authentication Max Count** – The number of times the switch will attempt to re-authenticate a connected client before the port becomes unauthorized.

Web – Click dot1x, dot1x Information.

dot1X Information	
dot1X Re-authentication	Disabled
dot1X Max Request Count	2
Timeout for Quiet Period	60 seconds
Timeout for Re-authentication Period	3600 seconds
Timeout for Tx Period	30 seconds
Supplicant timeout	30 seconds
Server timeout	30 seconds
Re-authentication Max Count	2

CLI – This example shows the default protocol settings for dot1x. For a description of the additional entries displayed in the CLI, See “show dot1x” on page 72.

Console#show dot1x				4-72
Global 802.1X Parameters				
reauth-enabled:	yes			
reauth-period:	300			
quiet-period:	350			
tx-period:	300			
supp-timeout:	30			
server-timeout:	30			
reauth-max:	2			
max-req:	2			
802.1X Port Summary				
Port Name	Status	Mode	Authorized	
1	disabled	ForceAuthorized	n/a	
2	disabled	ForceAuthorized	n/a	
:				
25	disabled	ForceAuthorized	yes	
26	enabled	Auto	yes	

```

802.1X Port Details

802.1X is disabled on port 1
:
802.1X is enabled on port 26
Max request          2
Quiet period         350
Reauth period        300
Tx period            300
Status               Unauthorized
Port-control         Auto
Supplicant            00-00-00-00-00-00

Authenticator State Machine
State                Connecting
Reauth Count         3
Backend State Machine
State                Idle
Request Count        0
Identifier(Server)   0

Reauthentication State Machine
State                Initialize
Console#

```

Configuring 802.1x Global Settings

The dot1x protocol includes global parameters that control the client authentication process that runs between the client and the switch (i.e., authenticator), as well as the client identity lookup process that runs between the switch and authentication server. The configuration options for parameters are described in this section.

Command Attributes

- **dot1X Re-authentication** – Sets the client to be re-authenticated after the interval specified by the Timeout for Re-authentication Period. Re-authentication can be used to detect if a new device is plugged into a switch port. (Default: Disabled)
- **dot1X Max Request Count** – Sets the maximum number of times the switch port will retransmit an EAP request packet to the client before it times out the authentication session. (Range: 1-10; Default 2)

- **Timeout for Quiet Period** – Sets the time that a switch port waits after the dot1X Max Request Count has been exceeded before attempting to acquire a new client. (Range: 1-65535 seconds; Default: 60 seconds)
- **Timeout for Re-authentication Period** – Sets the time period after which a connected client must be re-authenticated. (Range: 1-65535 seconds; Default: 3600 seconds)
- **Timeout for TX Period** – Sets the time period during an authentication session that the switch waits before re-transmitting an EAP packet. (Range: 1-65535; Default: 30 seconds)
- **authentication dot1x default*** – Sets the default authentication server type. Note that the specified authentication server type must be enabled and properly configured for dot1x to function properly. (Options: radius).

* CLI only.

Web – Select dot1X, dot1X Configuration. Enable dot1x globally for the switch, modify any of the parameters required, and then click Apply.

dot1X Configuration

dot1X Re-authentication	<input type="checkbox"/> Enable	
dot1X Max Request Count (1-10)	2	
Timeout for Quiet Period (0-65535)	60	seconds
Timeout for Re-authentication Period (0-65535)	3600	seconds
Timeout for Tx Period (1-65535)	30	seconds

CLI – This example enables re-authentication and sets all of the global parameters for dot1x.

Console(config)#dot1x re-authentication	4-69
Console(config)#dot1x max-req 5	4-68
Console(config)#dot1x timeout quiet-period 40	4-70
Console(config)#dot1x timeout re-auth 5	4-70
Console(config)#dot1x timeout tx-period 40	4-71
Console(config)#authentication dot1x default radius	4-67
Console(config)#	

Configuring Port Authorization Mode

When dot1x is enabled, you need to specify the dot1x authentication mode configured for each port.

Command Attributes

- **Status** – Indicates if authentication is enabled or disabled on the port.
- **Mode** – Sets the authentication mode to one of the following options:
 - **Auto** – Requires a dot1x-aware client to be authorized by the authentication server. Clients that are not dot1x-aware will be denied access.
 - **Force-Authorized** – Forces the port to grant access to all clients, either dot1x-aware or otherwise.
 - **Force-Unauthorized** – Forces the port to deny access to all clients, either dot1x-aware or otherwise.
- **Authorized** –
 - **Yes** – Connected client is authorized.
 - **No** – Connected client is not authorized.
 - *Blank* – Displays nothing when dot1x is disabled on a port.
- **Supplicant** – Indicates the MAC address of a connected client.
- **Trunk** – Indicates if the port is configured as a trunk port.

Web – Click dot1X, dot1X Port configuration. Select the authentication mode from the drop-down box and click Apply.

Port	Status	Mode	Authorized	Supplicant	Trunk
1	Enabled	Force-Unauthorized	No	00-00-00-00-00-00	
2	Disabled	Force-Authorized		00-00-00-00-00-00	
3	Disabled	Force-Authorized		00-00-00-00-00-00	
4	Enabled	Auto	No	00-00-E8-98-73-21	
5	Disabled	Force-Authorized		00-00-00-00-00-00	

CLI – This example sets the authentication mode to enable dot1x on port 2.

Console(config)#interface ethernet 1/2	4-119
Console(config-if)#dot1x port-control auto	4-68
Console(config-if)#	

Displaying 802.1x Statistics

This switch can display statistics for dot1x protocol exchanges for any port.

Statistical Values

Parameter	Description
Rx EXPOL Start	The number of EAPOL Start frames that have been received by this Authenticator.
Rx EAPOL Logoff	The number of EAPOL Logoff frames that have been received by this Authenticator.
Rx EAPOL Invalid	The number of EAPOL frames that have been received by this Authenticator in which the frame type is not recognized.
Rx EAPOL Total	The number of valid EAPOL frames of any type that have been received by this Authenticator.
Rx EAP Resp/Id	The number of EAP Resp/Id frames that have been received by this Authenticator.
Rx EAP Resp/Oth	The number of valid EAP Response frames (other than Resp/Id frames) that have been received by this Authenticator.
Rx EAP LenError	The number of EAPOL frames that have been received by this Authenticator in which the Packet Body Length field is invalid.
Rx Last EAPOLVer	The protocol version number carried in the most recently received EAPOL frame.
Rx Last EAPOLSrc	The source MAC address carried in the most recently received EAPOL frame.
Tx EAPOL Total	The number of EAPOL frames of any type that have been transmitted by this Authenticator.

Parameter	Description
Tx EAP Req/Id	The number of EAP Req/Id frames that have been transmitted by this Authenticator.
Tx EAP Req/Oth	The number of EAP Request frames (other than Rq/Id frames) that have been transmitted by this Authenticator.

Web – Select dot1X, dot1X Statistics. Select the required port and then click Query. Click Refresh to update the statistics.

dot1X Statistics

Port 4

Query

Rx EXPOL Start	2	Rx EAP LenError	0
Rx EAPOL Logoff	0	Rx Last EAPOLVer	1
Rx EAPOL Invalid	0	Rx Last EAPOLSrc	00-00-E8-98-73-21
Rx EAPOL Total	1022	Tx EAPOL Total	2047
Rx EAP Resp/Id	682	Tx EAP Resp/Id	1020
Rx EAP Resp/Oth	0	Tx EAP Resp/Oth	0

Refresh

CLI – This example displays the dot1x statistics for port 4.

```

Console#show dot1x statistics interface ethernet 1/4
4-72

Eth 1/4
Rx:  EXPOL      EAPOL      EAPOL      EAPOL      EAP      EAP      EAP
    Start      Logoff    Invalid    Total    Resp/Id  Resp/Oth  LenError
        2          0         0       1007       672         0         0

        Last      Last
EAPOLVer  EAPOLSrc
        1      00-00-E8-98-73-21

Tx:  EAPOL      EAP
    Total      Req/Id    Req/Oth
       2017     1005         0
Console#

```


Access Control Lists

Access Control Lists (ACL) provide packet filtering for IP frames (based on address, protocol, TCP/UDP port number or TCP control code) or any frames (based on MAC address or Ethernet type). To filter incoming packets, first create an access list, add the required rules, and then bind the list to a specific port.

Configuring Access Control Lists

An ACL is a sequential list of permit or deny conditions that apply to IP addresses, MAC addresses, or other more specific criteria. This switch tests incoming packets against the conditions in an ACL one by one. If a list contains all permit rules, a packet will be accepted as soon as it passes any of the rules. If a list contains all deny rules, a packet will be rejected as soon as it fails any one of the rules. In other words, if no rules match for a permit list, the packet is dropped; and if no rules match for a deny list, the packet is accepted.

Command Usage

The following restrictions apply to ACLs:

- Each ACL can have up to 32 rules.
- The maximum number of ACLs is also 32.
- However, due to resource restrictions, the average number of rules bound to the ports should not exceed 20.
- The switch does not support the explicit “deny any any” rule for the IP ACL or MAC ACL. If these rules are included in an ACL, and you attempt to bind the ACL to an interface, the bind operation will fail.
- An access list can only contain all permit rules or all deny rules. In other words, for performance reasons, you cannot mix permit and deny rules in the same list.

The order in which active ACLs are checked is as follows:

1. User-defined rules in the MAC ACL.
2. User-defined rules in the IP ACL.
3. Explicit default rule (permit any any) in the IP ACL.
4. Explicit default rule (permit any any) in the MAC ACL.
5. If no explicit rule is matched, the implicit default is permit all.

Setting the ACL Name and Type

Use the ACL Configuration page to designate the name and type of an ACL.

Command Attributes

ACL Configuration – Setting the Name and Type

- **Name** – Name of the ACL. (Maximum length: 16 characters)
- **Type** – There are three filtering modes:
 - Standard: IP ACL mode that filters packets based on the source IP address.
 - Extended: IP ACL mode that filters packets based on source or destination IP address, as well as protocol type and protocol port number. If the “TCP” protocol type is specified, then you can also filter packets based on the TCP control code.
 - MAC: MAC ACL mode that filters packets based on the source or destination MAC address and the Ethernet frame type (RFC 1060).

Web – Click ACL, ACL Configuration. Enter an ACL name in the Name field, select the list type (IP Standard, IP Extended, or MAC), and click Add to open the configuration page for the new list.

ACL Configuration

Type	Name	Remove	Edit
<div style="display: flex; align-items: flex-start;"> <div style="margin-right: 10px;"> Name <input style="width: 100%;" type="text" value="david"/> Type Standard ▼ </div> <div style="margin-top: 20px;"> <input type="button" value="Add"/> </div> </div>			

CLI – This example creates a standard IP ACL named bill.

```
Console(config)#access-list ip standard bill
Console(config-std-acl)#
```

4-76

Configuring a Standard IP ACL

Command Attributes

- **Action** – An ACL can contain all permit rules or all deny rules.
(Default: Permit rules)
- **IP** – Specifies the source IP address. Use “Any” to include all possible addresses, “Host” to specify a specific host address in the Address field, or “IP” to specify a range of addresses with the Address and SubMask fields. (Options: Any, Host, IP; Default: Any)
- **Address** – Source IP address.
- **SubMask** – A subnet mask containing four integers from 0 to 255, each separated by a period. The mask uses 1 bits to indicate “match” and 0 bits to indicate “ignore.” The mask is bitwise ANDed with the specified source IP address, and compared with the address for each IP packet entering the port(s) to which this ACL has been assigned.

Web – Specify the action (i.e., Permit or Deny). Select the address type (Any, Host, or IP). If you select “Host,” enter a specific address. If you select “IP,” enter a subnet address and the mask for an address range. Then click Add.

Standard ACL

Name: david

Action	Address	SubMask	Remove
Permit	10.1.1.21	255.255.255.255	<div>Remove</div>

IP

Ip

Address168.92.16.0

SubMask255.255.240.0

Add

CLI – This example configures one permit rule for the specific address 10.1.1.21 and another rule for the address range 168.92.16.x – 168.92.31.x using a bitmask..

Console(config-std-acl)#permit host 10.1.1.21

Console(config-std-acl)#permit 168.92.16.0 255.255.240.0

Console(config-std-acl)#

4-78

Configuring an Extended IP ACL

Command Attributes

- **Action** – An ACL can contain all permit rules or all deny rules. (Default: Permit rules)
- **Src/Dst IP** – Specifies the source or destination IP address. Use “Any” to include all possible addresses, “Host” to specify a specific host address in the Address field, or “IP” to specify a range of addresses with the Address and SubMask fields. (Options: Any, Host, IP; Default: Any)
- **Src/Dst Address** – Source or destination IP address.

- **Src/Dst SubMask** – Subnet mask for source or destination address.
(See SubMask in the preceding section.)
- **Protocol** – Specifies the protocol type to match as TCP, UDP or Others, where others indicates a specific protocol number (0-255).
(Options: TCP, UDP, Others; Default: TCP)
- **Src/Dst Port** – TCP or UDP source/destination port number.
(Range: 0-65535)
- **Control Code** – Decimal number (representing a bit string) that specifies flag bits in byte 14 of the TCP header. (Range: 0-63)
- **Control Bitmask** – Decimal number representing the code bits to match.

The control bitmask is a decimal number (for an equivalent binary bit mask) that is applied to the control code. Enter a decimal number, where the equivalent binary bit “1” means to match a bit and “0” means to ignore a bit. The following bits may be specified:

- 1 (fin) – Finish
- 2 (syn) – Synchronize
- 4 (rst) – Reset
- 8 (psh) – Push
- 16 (ack) – Acknowledgement
- 32 (urg) – Urgent pointer

For example, use the code value and mask below to catch packets with the following flags set:

- SYN flag valid, use “control-code 2 2”
- Both SYN and ACK valid, use “control-code 18 18”
- SYN valid and ACK invalid, use “control-code 2 18”

Web – Specify the action (i.e., Permit or Deny). Specify the source and/or destination addresses. Select the address type (Any, Host, or IP). If you select “Host,” enter a specific address. If you select “IP,” enter a subnet address and the mask for an address range. Set any other required criteria, such as service type, protocol type, or TCP control code. Then click Add.

Extend ACL

Name: mike

Action	Src Address	Src Mask	Dst Address	Dst Mask	Protocol	Src Port	Dst Port	Control Code	Control BitMask	Remove
Permit	10.7.1.0	255.255.255.0	Any	Any	6	Any	Any	Any	Any	<button>Remove</button>
Permit	192.168.1.0	255.255.255.0	Any	Any	6	Any	80	Any	Any	<button>Remove</button>

Src IP

Src Address

Src SubMask

Dst IP

Dst Address

Src SubMask

Protocol ☒ TCP(6) ☐ UDP(17) ☐ Others

Src Port

Dst Port

Control Code

Control BitMask

Add

CLI – This example adds three rules:

1. Accept any incoming packets if the source address is in subnet 10.7.1.x.
For example, if the rule is matched; i.e., the rule (10.7.1.0 & 255.255.255.0) equals the masked address (10.7.1.2 & 255.255.255.0), the packet passes through.
2. Allow TCP packets from class C addresses 192.168.1.0 to any destination address when set for destination TCP port 80 (i.e., HTTP).

3. Permit all TCP packets from class C addresses 192.168.1.0 with the TCP control code set to “SYN.”

```
Console(config-ext-acl)#permit 10.7.1.1 255.255.255.0 any 4-79
Console(config-ext-acl)#permit 192.168.1.0 255.255.255.0 any
dport 80
Console(config-ext-acl)#permit 192.168.1.0 255.255.255.0 any tcp
control-code 2 2
Console(config-std-acl)#
```

Configuring a MAC ACL

Command Usage

Egress MAC ACLs only work for destination-mac-known packets, not for multicast, broadcast, or destination-mac-unknown packets.

Command Attributes

- **Action** – An ACL can contain all permit rules or all deny rules.
(Default: Permit rules)
- **Source/Destination MAC** – Source or destination MAC address.
- **Source/Destination Mask** – Binary mask for source or destination MAC address.
- **Ethernet Type** – This option can only be used to filter Ethernet II formatted packets. (Range: 600-fff hex.)

A detailed listing of Ethernet protocol types can be found in RFC 1060.

A few of the more common types include 0800 (IP), 0806 (ARP), 8137 (IPX).

- **Packet Format** – This attribute includes the following packet types:
 - **Any** – Any Ethernet packet type.
 - **Untagged-eth2** – Untagged Ethernet II packets.
 - **Untagged-802.3** – Untagged Ethernet 802.3 packets.
 - **Tagged-eth2** – Tagged Ethernet II packets.
 - **Tagged-802.3** – Tagged Ethernet 802.3 packets.

Web – Specify the action (i.e., Permit or Deny). Specify the source and/or destination addresses. Enter a specific address (e.g., 11-22-33-44-55-66). Or enter a base address and a hexadecimal bitmask for an address range. Set any other required criteria, such as Ethernet type, or packet format. Then click Add.

MAC ACL

Name: jerry

Action	Source MAC	Source Mask	Destination MAC	Destination Mask	Ethernet Type	Packet Format	Remove
--------	------------	-------------	-----------------	------------------	---------------	---------------	--------

Action

Permit

Source MAC

Source Mask

Destination MAC

00-e0-29-94-34-de

Destination Mask

Ethernet Type

800

Packet Format

Any

Add

CLI – This rule permits packets from any source MAC address to the destination address 00-e0-29-94-34-de where the Ethernet type is 0800.

```
Console(config-mac-acl)#permit any host 00-e0-29-94-34-de
ethertype 0800
Console(config-mac-acl)#
```

4-85

Binding a Port to an Access Control List

After configuring Access Control Lists (ACL), you can bind the ports that need to filter traffic to the appropriate ACLs. You can only assign one IP access list and/or one MAC access list to any port.

Command Attributes

- **Port** – Fixed port or module. (Range: 1-26)
- **IP** – Specifies the IP ACL to bind to a port.
- **MAC** – Specifies the MAC ACL to bind to a port.

Web – Click ACL, ACL Port Binding. Mark the Enable field for the port you want to bind to an ACL, select the required ACL from the drop-down list, then click Apply.

ACL Port Binding					
Port	IP		MAC		Trunk
1	<input checked="" type="checkbox"/> Enable	david	<input checked="" type="checkbox"/> Enable	jerry	
2	<input checked="" type="checkbox"/> Enable	david	<input type="checkbox"/> Enable	jerry	
3	<input type="checkbox"/> Enable	david	<input type="checkbox"/> Enable	jerry	
4	<input type="checkbox"/> Enable	david	<input type="checkbox"/> Enable	jerry	
5	<input type="checkbox"/> Enable	david	<input type="checkbox"/> Enable	jerry	

CLI – This examples assigns an IP and MAC access list to port 1, and an IP access list to port 2.

```

Console(config)#interface ethernet 1/1
Console(config-if)#ip access-group david in
Console(config-if)#mac access-group jerry in
Console(config-if)#exit
Console(config)#interface ethernet 1/2
Console(config-if)#ip access-group david in
Console(config-if)#
  
```

Simple Network Management Protocol

Simple Network Management Protocol (SNMP) is a communication protocol designed specifically for managing devices on a network. Equipment commonly managed with SNMP includes switches, routers and host computers. SNMP is typically used to configure these devices for proper operation in a network environment, as well as to monitor them to evaluate performance or detect potential problems.

The switch includes an onboard SNMP agent that continuously monitors the status of its hardware, as well as the traffic passing through its ports. A network management station can access this information using software such as SMC's EliteView. Access rights to the onboard agent are controlled by community strings. To communicate with the switch, the management station must first submit a valid community string for authentication. The options for configuring community strings and related trap functions are described in the following sections.

Setting Community Access Strings

You may configure up to five community strings authorized for management access. All community strings used for IP Trap Managers should be listed in this table. For security reasons, you should consider removing the default strings.

Command Attributes

- **SNMP Community Capability** – Indicates that the switch supports up to five community strings.
- **Community String** – A community string that acts like a password and permits access to the SNMP protocol.

Default strings: “public” (read-only), “private” (read/write)

Range: 1-32 characters, case sensitive

- **Access Mode**

- **Read-Only** – Specifies read-only access. Authorized management stations are only able to retrieve MIB objects.
- **Read/Write** – Specifies read-write access. Authorized management stations are able to both retrieve and modify MIB objects.

Web – Click SNMP, SNMP Configuration. Add new community strings as required, select the access rights from the Access Mode drop-down list, then click Add.

The image shows a web-based configuration window titled "SNMP Configuration". It has a section for "SNMP Community:" and "SNMP Community Capability: 5". Below this, there are two columns: "Current:" and "New:". The "Current:" column contains a list box with "private RW" and "public RO". The "New:" column contains a "Community String" text box with "spiderman" entered, an "Access Mode" dropdown menu set to "Read/Write", and a "Read/Write" button. There are also "<< Add" and "Remove" buttons between the two columns.

CLI – The following example adds the string “spiderman” with read/write access.

```
Console(config)#snmp-server community spiderman rw
Console(config)#
```

4-90

Specifying Trap Managers and Trap Types

Traps indicating status changes are issued by the switch to specified trap managers. You must specify trap managers so that key events are reported by this switch to your management station (using network management platforms such as SMC’s EliteView). You can specify up to five management stations that will receive authentication failure messages and other trap messages from the switch.

Command Usage

- You can enable or disable authentication messages via the Web interface.
- You can enable or disable authentication messages or link-up-down messages via the CLI.

Command Attributes

- **Trap Manager Capability** – This switch supports up to five trap managers.
- **Trap Manager IP Address** – Internet address of the host (the targeted recipient).
- **Trap Manager Community String** – Community string sent with the notification operation. (Range: 1-32 characters, case sensitive)
- **Enable Authentication Traps** – Issues a trap message whenever an invalid community string is submitted during the SNMP access authentication process.

Web – Click SNMP, SNMP Configuration. Fill in the IP address and community string box for each Trap Manager that will receive these messages, mark Enable Authentication Traps if required, and then click Add.

The screenshot shows a web interface titled "Trap Managers:". Below the title, it says "Trap Manager Capability: 5". There are two columns: "Current:" and "New:". The "Current:" column has a dropdown menu showing "(none)". The "New:" column has two input fields: "Trap Manager IP address" with the value "10.1.19.23" and "Trap Manager Community String" with the value "batman". Between the columns are two buttons: "<< Add" and "Remove". At the bottom, there is a checkbox labeled "Enable Authentication Traps:" which is checked.

CLI – This example adds a trap manager and enables authentication traps.

Console(config)#snmp-server host 10.1.19.23 batman	4-93
Console(config)#snmp-server enable traps authentication	4-94

Dynamic Host Configuration Protocol

Dynamic Host Configuration Protocol (DHCP) can dynamically allocate an IP address and other configuration information to network clients when they boot up. If a subnet does not already include a BOOTP or DHCP server, you can relay DHCP client requests to a DHCP server on another subnet, or configure the DHCP server on this switch to support that subnet.

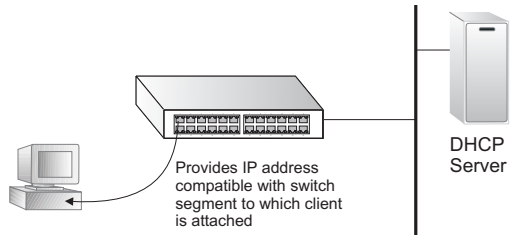
When configuring the DHCP server on this switch, you can configure an address pool for each unique IP interface, or manually assign a static IP address to clients based on their hardware address or client identifier. The DHCP server can provide the host's IP address, domain name, gateway router and DNS server, information about the host's boot image including the TFTP server to access for download and the name of the boot file, or boot information for NetBIOS Windows Internet Naming Service (WINS).

Configuring DHCP Relay Service

This switch supports DHCP relay service for attached host devices.

If DHCP relay is enabled, and this switch sees a DHCP request broadcast, it inserts its own IP

address into the request so that the DHCP server will know the subnet where the client is located. Then, the switch forwards the packet to the DHCP server. When the server receives the DHCP request, it allocates a free IP address for the DHCP client from its defined scope for the DHCP client's subnet, and sends a DHCP response back to the DHCP relay agent (i.e., this switch). This switch then broadcasts the DHCP response received from the server to the client.



Command Usage

You must specify the IP address for at least one DHCP server. Otherwise, the switch's DHCP relay agent will not forward client requests to a DHCP server.

Command Attributes

- **VLAN ID** – ID of configured VLAN.
- **VLAN Name** – Name of the VLAN.
- **Server IP Address** – Addresses of DHCP servers to be used by the switch's DHCP relay agent in order of preference.

Web – Click DHCP, Relay Configuration. Enter up to five IP addresses for any VLAN, then click Restart DHCP Relay to start the relay service.

Relay Configuration

VLAN ID	VLAN Name	Server IP Address			
1	DefaultVlan	10.1.0.99	0.0.0.0	0.0.0.0	0.0.0.0
		0.0.0.0			

Restart DHCP Relay

CLI – This example specifies one DHCP relay server for VLAN 1, and enables the relay service.

```

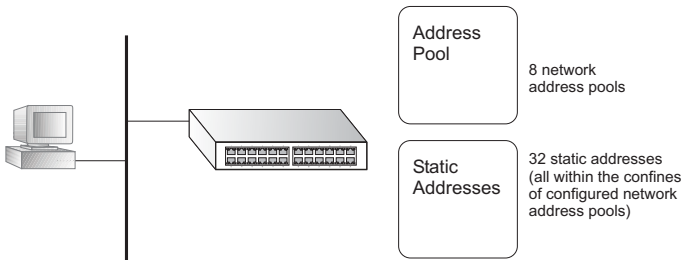
Console(config)#interface vlan 1                                4-119
Console(config-if)#dhcp relay server 10.1.0.99                 4-101
Console(config-if)#ip dhcp relay                               4-99
Console(config-if)#

```

Configuring the DHCP Server

This switch includes a Dynamic Host Configuration Protocol (DHCP) server that can assign temporary IP addresses to any attached host requesting service. It can also provide other network settings such as the domain name, default gateway, Domain Name Servers (DNS), Windows Internet Naming Service (WINS) name servers, or information on the bootstrap file for the host device to download.

Addresses can be assigned to clients from a common address pool configured for a specific IP interface on this switch, or fixed addresses can be assigned to hosts based on the client identifier code or MAC address.



Command Usage

- First configure any excluded addresses, including the address for this switch.
- Then configure address pools for the network interfaces. You can configure up to 8 network address pools. You can also manually bind an address to a specific client if required. However, any fixed addresses must fall within the range of an existing network address pool. You can configure up to 32 fixed host addresses (i.e., entering one address per pool).

Enabling the Server, Setting Excluded Addresses

Enable the DHCP Server and specify the IP addresses that it should not be assigned to clients.

Command Attributes

- **DHCP Server** – Enables or disables the DHCP server on this switch. (Default: Disabled)
- **Excluded Addresses** – Specifies IP addresses that the DHCP server should not assign to DHCP clients. You can specify a single address or an address range.

Note: Be sure you exclude the address for this switch and other key network devices.

Web – Click DHCP, Server, General. Enter a single address or an address range, and click Add.

General

DHCP Server: Enabled

Excluding Address:

10.1.0.250 ~ 10.1.0.254

<< Add

Remove

New:

Low:

High:

(optional)

Entry Count: 1

CLI – This example enables the DHCP and sets an excluded address range.

Console(config)#service dhcp4-103

Console(config)#ip dhcp excluded-address 10.1.0.2504-104

10.1.0.254

Console#

Configuring Address Pools

You must configure IP address pools for each IP interface that will provide addresses to attached clients via the DHCP server.

Command Usage

- First configure address pools for the network interfaces. Then you can manually bind an address to a specific client if required. However, note that any static host address must fall within the range of an existing network address pool. You can configure up to 8 network address pools, and up to 32 manually bound host address pools (i.e., one address per host pool).
- When a client request is received, the switch first checks for a network address pool matching the gateway where the request originated (i.e., if the request was forwarded by a relay server). If there is no gateway in the client request (i.e., the request was not forwarded by a relay server), the switch searches for a network pool matching the interface through which the client request was received. It then searches for a manually configured host address that falls within the matching network pool. If no manually configured host address is found, it assigns an address from the matching network address pool. However, if no matching address pool is found the request is ignored.
- When searching for a manual binding, the switch compares the client identifier and then the hardware address for DHCP clients. Since BOOTP clients cannot transmit a client identifier, you must configure a hardware address for this host type. If no manual binding has been specified for a host entry with a hardware address or client identifier, the switch will assign an address from the first matching network pool.
- If the subnet mask is not specified for network or host address pools, the class A, B, or C natural mask is used (see page 3-178). The DHCP server assumes that all host addresses are available. You can exclude subsets of the address space by using the IP Excluded Address field on the DHCP Server General configuration page.

Command Attributes

Creating a New Address Pool

- **Pool Name** – A string or integer. (Range: 1-8 characters)

Setting the Network Parameters

- **IP** – The IP address of the DHCP address pool.
- **Subnet Mask** – The bit combination that identifies the network (or subnet) and the host portion of the DHCP address pool.

Setting the Host Parameters

- **IP** – The IP address of the DHCP address pool.
- **Subnet Mask** – Specifies the network mask of the client.
- **Hardware Address** – Specifies the MAC address and protocol used on the client. (Options: Ethernet, IEEE802, FDDI; Default: Ethernet)
- **Client-Identifier** – A unique designation for the client device, either a text string (1-15 characters) or hexadecimal value.

Setting the Optional Parameters

- **Default Router** – The IP address of the primary and alternate gateway router. The IP address of the router should be on the same subnet as the client.
- **DNS Server** – The IP address of the primary and alternate DNS server. DNS servers must be configured for a DHCP client to map host names to IP addresses.
- **Netbios Server** – IP address of the primary and alternate NetBIOS Windows Internet Naming Service (WINS) name server used for Microsoft DHCP clients.
- **Netbios Type** – NetBIOS node type for Microsoft DHCP clients. (Options: Broadcast, Hybrid, Mixed, Peer to Peer; Default: Hybrid)
- **Domain Name** – The domain name of the client. (Range: 1-32 characters)

- **Bootfile** – The default boot image for a DHCP client. This file should be placed on the Trivial File Transfer Protocol (TFTP) server specified as the Next Server.
- **Next Server** – The IP address of the next server in the boot process, which is typically a Trivial File Transfer Protocol (TFTP) server.
- **Lease Time** – The duration that an IP address is assigned to a DHCP client. (Options: fixed period, Infinite; Default: 1 day)

Examples

Creating a New Address Pool

Web – Click DHCP, Server, Pool Configuration. Specify a pool name, then click Add.

Pool Configuration

Pool Name:

Pool Name	Type	IP	Mask	Configure	Delete
tps	Network	10.1.0.0	255.255.255.0	<input type="button" value="Configure"/>	<input type="button" value="Delete"/>

Entry Count: 1

CLI – This example adds an address pool and enters DHCP pool configuration mode.

```
Console(config)#ip dhcp pool mgr
Console(config-dhcp)#
```

4-104

Configuring a Network Address Pool

Web – Click DHCP, Server, Pool Configuration. Click the Configure button for any entry. Click the radio button for “Network.” Enter the IP address and subnet mask for the network pool. Configure the optional parameters such as default router and DNS server. Then click Apply.

Pool Name : **tps** >>
[Go back to Pool Configure](#)

☒ Network

IP
Subnet Mask

☐ Host

IP
Subnet Mask
Hardware Address
Client-Identifier

<<Option>>

Default Router
Default Router2 (optional)

DNS Server
DNS Server2 (optional)

Netbios Server
Netbios Server2 (optional)

Netbios type

Domain Name

Bootfile

Next Server

Lease time
☐ day hour min
☒ Infinite

CLI – This example configures a network address pool.

```

Console(config)#ip dhcp pool tps                                4-104
Console(config-dhcp)#network 10.1.0.0 255.255.255.0            4-105
Console(config-dhcp)#default-router 10.1.0.253                 4-106
Console(config-dhcp)#dns-server 10.2.3.4                       4-108
Console(config-dhcp)#netbios-name-server 10.1.0.33             4-110
Console(config-dhcp)#netbios-node-type hybrid                   4-111
Console(config-dhcp)#domain-name example.com                   4-107
Console(config-dhcp)#bootfile wme.bat                           4-109
Console(config-dhcp)#next-server 10.1.0.21                     4-109
Console(config-dhcp)#lease infinite                             4-112
Console(config-dhcp)#

```

Configuring a Host Address Pool

Web – Click DHCP, Server, Pool Configuration. Click the Configure button for any entry. Click the radio button for “Host.” Enter the IP address, subnet mask, and hardware address for the client device. Configure the optional parameters such as gateway server and DNS server. Then click Apply.

Pool Name : mgr >>
[Go back to Pool Configure](#)

☐ Network

IP
Subnet Mask

☒ Host

IP

10.1.0.19

Subnet Mask

255.255.255.0

Hardware Address

00-10-B5-51-69-F7

Ethernet

Client-Identifier

bear

Text

<<Option>>

Default Router

10.1.0.253

Default Router2

(optional)

DNS Server

10.2.3.4

DNS Server2

(optional)

Netbios Server

10.1.0.33

Netbios Server2

(optional)

Netbios type

Hybrid

Domain Name

example.com

Bootfile

pc9.bet

Next Server

10.1.0.21

Lease time

☐ day
 hour
 min

☒ Infinite

CLI – This example configures a host address pool.

Console(config)#ip dhcp pool mgr	4-104
Console(config-dhcp)#host 10.1.0.19 255.255.255.0	4-113
Console(config-dhcp)#hardware-address 00-e0-29-94-34-28 ethernet	4-115
Console(config-dhcp)#client-identifier text bear	4-114
Console(config-dhcp)#default-router 10.1.0.253	4-106
Console(config-dhcp)#dns-server 10.2.3.4	4-108
Console(config-dhcp)#netbios-name-server 10.1.0.33	4-110
Console(config-dhcp)#netbios-node-type hybrid	4-111
Console(config-dhcp)#domain-name example.com	4-107
Console(config-dhcp)#bootfile wme.bat	4-109
Console(config-dhcp)#next-server 10.1.0.21	4-109
Console(config-dhcp)#lease infinite	4-112
Console(config-dhcp)#	

Displaying Address Bindings

You can display the host devices which have acquired an IP address from this switch's DHCP server.

Command Attributes

- **IP Address** – IP address assigned to host.
- **Mac Address** – MAC address of host.
- **Lease time** – Duration that this IP address can be used by the host.
- **Start time** – Time this address was assigned by the switch.
- **Delete** – Clears this binding to the host. This command is normally used after modifying the address pool, or after moving DHCP service to another device.
- **Entry Count** – Number of hosts that have been given addresses by the switch.

Note: More than one DHCP server may respond to a service request by a host. In this case, the host generally accepts the first address assigned by any DHCP server.

Web – Click DHCP, Server, IP Binding. You may use the Delete button to clear an address from the DHCP server's database.

IP Binding

IP Address	Mac Address	Lease time	Start time	Delete
10.1.0.20	00-00-E8-98-73-21	2147483647	63829031	Delete

Entry Count: 1

CLI – This example displays the current binding, and then clears all automatic binding.

```

Console#show ip dhcp binding                                     4-117
      IP                MAC                Lease Time          Start
-----
      10.1.0.20 00-00-e8-98-73-21          86400 Dec 25 08:01:57 2002
Console#clear ip dhcp binding *                                4-116
Console#
  
```

Port Configuration

Displaying Connection Status

You can use the Port Information or Trunk Information pages to display the current connection status, including link state, speed/duplex mode, flow control, and auto-negotiation.

Field Attributes (Web)

- **Name** – Interface label.
- **Type** – Indicates the port type (100BASE-TX, 1000BASE-T, 1000BASE-SX, 1000BASE-LX or 100BASE-FX).
- **Admin Status** – Shows if the interface is enabled or disabled.
- **Oper Status** – Indicates if the link is Up or Down.

- **Speed/Duplex Status** – Shows the current speed and duplex mode. (Auto, or fixed choice)
- **Flow Control Status** – Indicates type of flow control currently in use. (IEEE 802.3x, Back-Pressure or None)
- **Autonegotiation** – Shows if auto-negotiation is enabled or disabled.
- **Trunk Member**¹ – Shows if port is a trunk member.
- **Creation**² – Shows if a trunk is manually configured or dynamically set via LACP.

1: Port Information only.

2: Trunk Information only

Web – Click Port, Port Information or Trunk Information.

Port Information								
Port	Name	Type	Admin Status	Oper Status	Speed Duplex Status	Flow Control Status	Autonegotiation	Trunk Member
1		100Base-TX	Enabled	Up	100full	None	Enabled	
2		100Base-TX	Enabled	Down	100full	None	Enabled	
3		100Base-TX	Enabled	Up	100full	None	Enabled	
4		100Base-TX	Enabled	Down	100full	None	Enabled	
5		100Base-TX	Enabled	Down	100full	None	Enabled	
6		100Base-TX	Enabled	Down	100full	None	Enabled	
7		100Base-TX	Enabled	Up	100full	None	Enabled	
8		100Base-TX	Enabled	Down	100full	None	Enabled	
9		100Base-TX	Enabled	Down	100full	None	Enabled	
10		100Base-TX	Enabled	Down	100full	None	Enabled	

Field Attributes (CLI)

Basic information:

- **Port type** – Indicates the port type. (1000BASE-T, 1000BASE-SX, 1000BASE-LX)
- **MAC Address** – The physical layer address for this port. (To access this item on the Web, see “Setting the Switch’s IP Address” on page 3-17.)

Configuration:

- **Name** – Interface label.
- **Port admin** – Shows if the interface is enabled or disabled (i.e., up or down).

- **Speed-duplex** – Shows the current speed and duplex mode. (Auto, or fixed choice)
- **Capabilities** – Specifies the capabilities to be advertised for a port during auto-negotiation. (To access this item on the Web, see “Configuring Interface Connections” on page 3-48.) The following capabilities are supported.
 - **10half** - Supports 10 Mbps half-duplex operation
 - **10full** - Supports 10 Mbps full-duplex operation
 - **100half** - Supports 100 Mbps half-duplex operation
 - **100full** - Supports 100 Mbps full-duplex operation
 - **1000full** - Supports 1000 Mbps full-duplex operation
 - **Sym** - Transmits and receives pause frames for flow control
 - **FC** - Supports flow control
- **Broadcast storm** – Shows if broadcast storm control is enabled or disabled.
- **Broadcast storm limit** – Shows the broadcast storm threshold. (500 - 262143 packets per second)
- **Flow control** – Shows if flow control is enabled or disabled.
- **LACP** – Shows if LACP is enabled or disabled.

Current status:

- **Link Status** – Indicates if the link is Up or Down.
- **Port Operation Status** – Provides detailed information on port state.
- **Operation speed-duplex** – Shows the current speed and duplex mode.
- **Flow control type** – Indicates the type of flow control currently in use. (IEEE 802.3x, Back-Pressure or none)

CLI – This example shows the connection status for Port 13.

```
Console#show interfaces status ethernet 1/13 4-128
Information of Eth 1/13
Basic information:
  Port type: 100tx
  Mac address: 00-30-f1-47-58-46
Configuration:
  Name:
  Port admin: Up
  Speed-duplex: Auto
  Capabilities: 10half, 10full, 100half, 100full,
  Broadcast storm: Enabled
  Broadcast storm limit: 500 packets/second
  Flow control: Disabled
  LACP: Disabled
Current status:
  Link status: Down
  Port operation status: Up
  Operation speed-duplex: 100full
  Flow control type: None
Console#
```

Configuring Interface Connections

You can use the Port Configuration or Trunk Configuration page to enable/disable an interface, set auto-negotiation and the interface capabilities to advertise, or manually fix the speed, duplex mode, and flow control.

Command Attributes

- **Name** – Allows you to label an interface. (Range: 1-64 characters)
- **Admin** – Allows you to manually disable an interface. You can disable an interface due to abnormal behavior (e.g., excessive collisions), and then reenable it after the problem has been resolved. You may also disable an interface for security reasons.
- **Speed/Duplex** – Allows you to manually set the port speed and duplex mode.
- **Flow Control** – Allows automatic or manual selection of flow control.
- **Autonegotiation** (Port Capabilities) – Allows auto-negotiation to be enabled/disabled. When auto-negotiation is enabled, you need to specify the capabilities to be advertised. When auto-negotiation is disabled, you can force the settings for speed, mode, and flow control. The following capabilities are supported.
 - **10half** - Supports 10 Mbps half-duplex operation
 - **10full** - Supports 10 Mbps full-duplex operation
 - **100half** - Supports 100 Mbps half-duplex operation
 - **100full** - Supports 100 Mbps full-duplex operation
 - **1000full** - Supports 1000 Mbps full-duplex operation
 - **Sym** (Gigabit only) - Check this item to transmit and receive pause frames, or clear it to auto-negotiate the sender and receiver for asymmetric pause frames. (*The current switch chip only supports symmetric pause frames.*)
 - **FC** - Supports flow control

Flow control can eliminate frame loss by “blocking” traffic from end stations or segments connected directly to the switch when its buffers fill. When enabled, back pressure is used for half-duplex operation and IEEE 802.3x for full-duplex operation. (Avoid using flow control on a

port connected to a hub unless it is actually required to solve a problem. Otherwise back pressure jamming signals may degrade overall performance for the segment attached to the hub.)

(Default: Autonegotiation enabled; Advertised capabilities for 100BASE-TX – 10half, 10full, 100half, 100full; 1000BASE-T – 10half, 10full, 100half, 100full, 1000full; 1000BASE-SX/LX/LH – 1000full)

- **Trunk** – Indicates if a port is a member of a trunk. To create trunks and select port members, see “Trunk Configuration” on page 3-79.

Note: Auto-negotiation must be disabled before you can configure or force the interface to use the Speed/Duplex Mode or Flow Control options.

Web – Click Port, Port Configuration or Trunk Configuration. Modify the required interface settings, and click Apply.

Port Configuration								
Port	Name	Admin	Speed Duplex	Flow Control	Autonegotiation			Trunk
1		<input checked="" type="checkbox"/> Enable	100full	Disabled	Enabled	<input checked="" type="checkbox"/> 10h <input checked="" type="checkbox"/> 100h <input type="checkbox"/> 1000h <input type="checkbox"/> Sym <input checked="" type="checkbox"/> 10f <input checked="" type="checkbox"/> 100f <input type="checkbox"/> 1000f <input type="checkbox"/> FC		
2		<input checked="" type="checkbox"/> Enable	100full	Disabled	Enabled	<input checked="" type="checkbox"/> 10h <input checked="" type="checkbox"/> 100h <input type="checkbox"/> 1000h <input type="checkbox"/> Sym <input checked="" type="checkbox"/> 10f <input checked="" type="checkbox"/> 100f <input type="checkbox"/> 1000f <input type="checkbox"/> FC		
3		<input checked="" type="checkbox"/> Enable	100full	Disabled	Enabled	<input checked="" type="checkbox"/> 10h <input checked="" type="checkbox"/> 100h <input type="checkbox"/> 1000h <input type="checkbox"/> Sym <input checked="" type="checkbox"/> 10f <input checked="" type="checkbox"/> 100f <input type="checkbox"/> 1000f <input type="checkbox"/> FC		

CLI – Select the interface, and then enter the required settings.

```

Console(config)#interface ethernet 1/13                                4-119
Console(config-if)#description RD SW#13                               4-119
Console(config-if)#shutdown                                           4-125
.
Console(config-if)#no shutdown
Console(config-if)#no negotiation                                    4-121
Console(config-if)#speed-duplex 100half                               4-120
Console(config-if)#flowcontrol                                        4-124
.
Console(config-if)#negotiation
Console(config-if)#capabilities 100half                               4-122
Console(config-if)#capabilities 100full
Console(config-if)#capabilities flowcontrol
    
```

Setting Broadcast Storm Thresholds

Broadcast storms may occur when a device on your network is malfunctioning, or if application programs are not well designed or properly configured. If there is too much broadcast traffic on your network, performance can be severely degraded or everything can come to complete halt.

You can protect your network from broadcast storms by setting a threshold for broadcast traffic for each port. Any broadcast packets exceeding the specified threshold will then be dropped.

Command Usage

- Broadcast Storm Control is enabled by default.
- The default threshold is 500 packets per second.
- Broadcast control does not effect IP multicast traffic.
- The specified threshold applies to all ports on the switch.

Command Attributes

- **Threshold** – Threshold as percentage of port bandwidth. (Options: 500-262143 packets per second; Default: 500 packets per second)
- **Broadcast Control Status** – Shows whether or not broadcast storm control has been enabled. (Default: Enabled)

Web – Click Port, Port Broadcast Control. Set the threshold for all ports, click Apply.

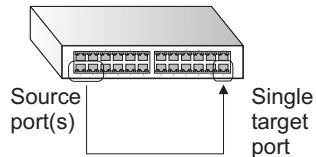
Broadcast Control	
Threshold (packets/sec)	600
Broadcast Control Status	Enabled ▼

CLI – Specify any interface, and then enter the threshold. The following sets broadcast suppression at 600 packets per second.

```
Console(config)#interface ethernet 1/1          4-119
Console(config-if)#switchport broadcast packet-rate 600  4-126
Console(config-if)#end
Console#show interfaces switchport ethernet 1/12        4-131
Information of Eth 1/12
Broadcast threshold: Enabled, 600 packets/second
Lacp status: Disabled
VLAN membership mode: Hybrid
Ingress rule: Disabled
Acceptable frame type: All frames
Native VLAN: 1
Priority for untagged traffic: 0
Gvrp status: Disabled
Allowed Vlan: 1(u),
Forbidden Vlan:
Console#
```

Configuring Port Mirroring

You can mirror traffic from any source port to a target port for real-time analysis. You can then attach a logic analyzer or RMON probe to the target port and study the traffic crossing the source port in a completely unobtrusive manner.



Command Usage

- Monitor port speed should match or exceed source port speed, otherwise traffic may be dropped from the monitor port.
- All mirror sessions have to share the same destination port.
- When mirroring port traffic, the target port must be included in the same VLAN as the source port.

Command Attributes

- **Mirror Sessions** – Displays a list of current mirror sessions.
- **Source Port** – The port whose traffic will be monitored.

- **Type** – Allows you to select which traffic to mirror to the target port, Rx (receive), Tx (transmit), or Both.
- **Target Port** – The port that will “duplicate” or “mirror” the traffic on the source port.

Web – Click Port, Mirror. Specify the source port, the traffic type to be mirrored, and the monitor port, then click Add.

CLI – Use the interface command to select the monitor port, then use the port monitor command to specify the source port. Note that default mirroring under the CLI is for both received and transmitted packets.

```
Console(config)#interface ethernet 1/10      4-119
Console(config-if)#port monitor ethernet 1/13 4-133
Console(config-if)#
```

Showing Port Statistics

You can display standard statistics on network traffic from the Interfaces Group and Ethernet-like MIBs, as well as a detailed breakdown of traffic based on the RMON MIB. Interfaces and Ethernet-like statistics display errors on the traffic passing through each port. This information can be used to identify potential problems with the switch (such as a faulty port or unusually heavy loading). RMON statistics provide access to a broad range of statistics, including a total count of different frame types and sizes

passing through each port. All values displayed have been accumulated since the last system reboot, and are shown as counts per second. Statistics are refreshed every 60 seconds by default.

Note: RMON groups 2, 3 and 9 can only be accessed using SNMP management software such as SMC's EliteView.

Statistical Values

Parameter	Description
<i>Interface Statistics</i>	
Received Octets	The total number of octets received on the interface, including framing characters.
Received Unicast Packets	The number of subnetwork-unicast packets delivered to a higher-layer protocol.
Received Multicast Packets	The number of packets, delivered by this sub-layer to a higher (sub-)layer, which were addressed to a multicast address at this sub-layer.
Received Broadcast Packets	The number of packets, delivered by this sub-layer to a higher (sub-)layer, which were addressed to a broadcast address at this sub-layer.
Received Discarded Packets	The number of inbound packets which were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol. One possible reason for discarding such a packet could be to free up buffer space.
Received Unknown Packets	The number of packets received via the interface which were discarded because of an unknown or unsupported protocol.
Received Errors	The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.
Transmit Octets	The total number of octets transmitted out of the interface, including framing characters.
Transmit Unicast Packets	The total number of packets that higher-level protocols requested be transmitted to a subnetwork-unicast address, including those that were discarded or not sent.

Parameter	Description
Transmit Multicast Packets	The total number of packets that higher-level protocols requested be transmitted, and which were addressed to a multicast address at this sub-layer, including those that were discarded or not sent.
Transmit Broadcast Packets	The total number of packets that higher-level protocols requested be transmitted, and which were addressed to a broadcast address at this sub-layer, including those that were discarded or not sent.
Transmit Discarded Packets	The number of outbound packets which were chosen to be discarded even though no errors had been detected to prevent their being transmitted. One possible reason for discarding such a packet could be to free up buffer space.
Transmit Errors	The number of outbound packets that could not be transmitted because of errors.
<i>Etherlike Statistics</i>	
Alignment Errors	The number of alignment errors (missynchronized data packets).
Late Collisions	The number of times that a collision is detected later than 512 bit-times into the transmission of a packet.
FCS Errors	A count of frames received on a particular interface that are an integral number of octets in length but do not pass the FCS check. This count does not include frames received with frame-too-long or frame-too-short error.
Excessive Collisions	A count of frames for which transmission on a particular interface fails due to excessive collisions. This counter does not increment when the interface is operating in full-duplex mode.
Single Collision Frames	The number of successfully transmitted frames for which transmission is inhibited by exactly one collision.
Internal MAC Transmit Errors	A count of frames for which transmission on a particular interface fails due to an internal MAC sublayer transmit error.

Parameter	Description
Multiple Collision Frames	A count of successfully transmitted frames for which transmission is inhibited by more than one collision.
Carrier Sense Errors	The number of times that the carrier sense condition was lost or never asserted when attempting to transmit a frame.
SQE Test Errors	A count of times that the SQE TEST ERROR message is generated by the PLS sublayer for a particular interface.
Frames Too Long	A count of frames received on a particular interface that exceed the maximum permitted frame size.
Deferred Transmissions	A count of frames for which the first transmission attempt on a particular interface is delayed because the medium was busy.
Internal MAC Receive Errors	A count of frames for which reception on a particular interface fails due to an internal MAC sublayer receive error.
<i>RMON Statistics</i>	
Drop Events	The total number of events in which packets were dropped due to lack of resources.
Jabbers	The total number of frames received that were longer than 1518 octets (excluding framing bits, but including FCS octets), and had either an FCS or alignment error.
Received Bytes	Total number of bytes of data received on the network. This statistic can be used as a reasonable indication of Ethernet utilization.
Collisions	The best estimate of the total number of collisions on this Ethernet segment.
Received Frames	The total number of frames (bad, broadcast and multicast) received.
Broadcast Frames	The total number of good frames received that were directed to the broadcast address. Note that this does not include multicast packets.
Multicast Frames	The total number of good frames received that were directed to this multicast address.

Parameter	Description
CRC/Alignment Errors	The number of CRC/alignment errors (FCS or alignment errors).
Undersize Frames	The total number of frames received that were less than 64 octets long (excluding framing bits, but including FCS octets) and were otherwise well formed.
Oversize Frames	The total number of frames received that were longer than 1518 octets (excluding framing bits, but including FCS octets) and were otherwise well formed.
Fragments	The total number of frames received that were less than 64 octets in length (excluding framing bits, but including FCS octets) and had either an FCS or alignment error.
64 Bytes Frames	The total number of frames (including bad packets) received and transmitted that were 64 octets in length (excluding framing bits but including FCS octets).
65-127 Byte Frames 128-255 Byte Frames 256-511 Byte Frames 512-1023 Byte Frames 1024-1518 Byte Frames 1519-1536 Byte Frames	The total number of frames (including bad packets) received and transmitted where the number of octets fall within the specified range (excluding framing bits but including FCS octets).

Web – Click Statistics, Port Statistics. Select the required interface, and click Query. You can also use the Refresh button at the bottom of the page to update the screen.

Port Statistics

Interface
☒ Port 1
☐ Trunk

Query

Interface Statistics:

Received Octets	15020	Received Unicast Packets	0
Received Multicast Packets	177	Received Broadcast Packets	0
Received Discarded Packets	0	Received Unknown Packets	0
Received Errors	0	Transmit Octets	168087
Transmit Unicast Packets	0	Transmit Multicast Packets	2420
Transmit Broadcast Packets	47	Transmit Discarded Packets	0
Transmit Errors	0		

Etherlike Statistics:

Alignment Errors	0	Late Collisions	0
FCS Errors	0	Excessive Collisions	0
Single Collision Frames	0	Internal MAC Transmit Errors	0
Multiple Collision Frames	0	Carrier Sense Errors	0
SOE Test Errors	0	Frames Too Long	0
Deferred Transmissions	0	Internal MAC Receive Errors	0

RMON Statistics:

Drop Events	0	Jabbers	0
Received Bytes	188155	Collisions	0
Received Frames	0	64 Bytes Frames	2249
Broadcast Frames	47	65-127 Bytes Frames	459
Multicast Frames	2672	128-255 Bytes Frames	11
CRC/Alignment Errors	0	256-511 Bytes Frames	0
Undersize Frames	0	512-1023 Bytes Frames	0
Oversize Frames	0	1024-1518 Bytes Frames	0
Fragments	0		

Refresh

CLI – This example shows statistics for port 13.

```

Console#show interfaces counters ethernet 1/13
Ethernet 1/13
Iftable stats:
  Octets input: 868453, Octets output: 3492122
  Unicast input: 7315, Unicast output: 6658
  Discard input: 0, Discard output: 0
  Error input: 0, Error output: 0
  Unknown protos input: 0, QLen output: 0
Extended iftable stats:
  Multi-cast input: 0, Multi-cast output: 17027
  Broadcast input: 231, Broadcast output: 7
Ether-like stats:
  Alignment errors: 0, FCS errors: 0
  Single Collision frames: 0, Multiple collision frames: 0
  SQE Test errors: 0, Deferred transmissions: 0
  Late collisions: 0, Excessive collisions: 0
  Internal mac transmit errors: 0, Internal mac receive errors: 0
  Frame too longs: 0, Carrier sense errors: 0
  Symbol errors: 0

RMON stats:
  Drop events: 0, Octets: 4422579, Packets: 31552
  Broadcast pkts: 238, Multi-cast pkts: 17033
  Undersize pkts: 0, Oversize pkts: 0
  Fragments: 0, Jabbers: 0
  CRC align errors: 0, Collisions: 0
  Packet size <= 64 octets: 25568, Packet size 65 to 127 octets:
    1616
  Packet size 128 to 255 octets: 1249, Packet size 256 to 511
    octets: 1449
  Packet size 512 to 1023 octets: 802, Packet size 1024 to 1518
    octets: 871

```

4-129

Configuring Rate Limits

This function allows the network manager to control the maximum rate for traffic transmitted or received on an interface. Rate limiting is configured on interfaces at the edge of a network to limit traffic into or out of the network. Traffic that falls within the rate limit is transmitted, while packets that exceed the acceptable amount of traffic are dropped.

Rate limiting can be applied to individual ports or trunks. When an interface is configured with this feature, the traffic rate will be monitored by the hardware to verify conformity. Non-conforming traffic is dropped, conforming traffic is forwarded without any changes.

Command Usage

Due to a switch chip limitation, the input rate limit can only be enabled or disabled globally for all interfaces on the switch. However, the output rate limit can be enabled or disabled for individual interfaces.

Command Attribute

- **Rate Limit** – Sets the input or output rate limit for an interface.

Default Status – Disabled

Default Rate – Fast Ethernet: 100 Mbps, Gigabit Ethernet: 1000 Mbps

Range – Fast Ethernet: 1 - 100 Mbps (at a resolution of 1 Mbps),

Gigabit Ethernet: 1 - 1000 Mbps (at an resolution of 8 Mbps)

Web - Click Rate Limit, Input/Output Rate Limit Port/Trunk Configuration. Set the Input Rate Limit Status (for all interfaces), or set the Output Rate Limit Status (for selected interfaces), then set the rate limit for individual interfaces, and click Apply.

Input Rate Limit Port Configuration

Input Rate Limit Status: Enabled

Port	Input Rate Limit(Mbps)	Trunk
1	60	
2		
3		
4		
5		
6		
7		
8		
9		
10		

Output Rate Limit Port Configuration

Port	Output Rate Limit Status	Output Rate Limit(Mbps)	Trunk
1	Enabled	60	
2	Disabled	100	
3	Disabled	100	
4	Disabled	100	
5	Disabled	100	
6	Disabled	100	
7	Disabled	100	
8	Disabled	100	

CLI - This example sets the rate limit for input and output traffic passing through port 1 to 60 Mbps.

Console(config)#interface ethernet 1/1	4-119
Console(config-if)#rate-limit input 60	4-136
Console(config-if)#rate-limit output 60	
Console(config-if)#	

Trunk Configuration

You can create multiple links between devices that work as one virtual, aggregate link. A port trunk offers a dramatic increase in bandwidth for network segments where bottlenecks exist, as well as providing a fault-tolerant link between two devices. You can create up to six trunks at a time.

The switch supports both static trunking and dynamic Link Aggregation Control Protocol (LACP). Static trunks have to be manually configured at both ends of the link, and the switches must comply with the Cisco EtherChannel standard. On the other hand, LACP configured ports can automatically negotiate a trunked link with LACP-configured ports on another device. You can configure any number of ports on the switch as LACP, as long as they are not already configured as part of a static trunk. If ports on another device are also configured as LACP, the switch and the other device will negotiate a trunk link between them. If an LACP trunk consists of more than four ports, all other ports will be placed in a standby mode. Should one link in the trunk fail, one of the standby ports will automatically be activated to replace it.

Command Usage

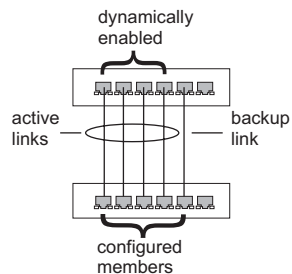
Besides balancing the load across each port in the trunk, the other ports provide redundancy by taking over the load if a port in the trunk fails. However, before making any physical connections between devices, use the Web interface or CLI to specify the trunk on the devices at both ends. When using a port trunk, take note of the following points:

- Finish configuring port trunks before you connect the corresponding network cables between switches to avoid creating a loop.
- You can create up to six trunks on the switch, with up to four ports per trunk.
- The ports at both ends of a connection must be configured as trunk ports.
- When configuring static trunks on switches of different types, they must be compatible with the Cisco EtherChannel standard.
- The ports at both ends of a trunk must be configured in an identical manner, including communication mode (i.e., speed, duplex mode and flow control), VLAN assignments, and CoS settings.
- All the ports in a trunk have to be treated as a whole when moved from/to, added or deleted from a VLAN.
- STP, VLAN, and IGMP settings can only be made for the entire trunk.

Dynamically Configuring a Trunk

Command Usage

- To avoid creating a loop in the network, be sure you enable LACP before connecting the ports, and also disconnect the ports before disabling LACP.
- If the target switch has also enabled LACP on the connected ports, the trunk will be activated automatically.



- A trunk formed with another switch using LACP will automatically be assigned the next available trunk ID.
- If more than four ports attached to the same target switch have LACP enabled, the additional ports will be placed in standby mode, and will only be enabled if one of the active links fails.
- All ports on both ends of an LACP trunk must be configured for full duplex, either by forced mode or auto-negotiation.

Web – Click Trunk, LACP Configuration. Select any of the switch ports from the scroll-down port list and click Add. After you have completed adding ports to the member list, click Apply.

LACP Configuration

Member List:

Current:

New:

Unit1 Port17
Unit1 Port18

<<Add

Remove

Port 1 ▾

CLI – The following example enables LACP for ports 17 and 18. Just connect these ports to two LACP-enabled trunk ports on another switch to form a trunk.

```

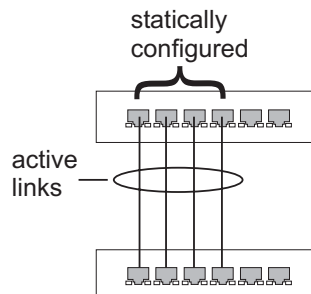
Console(config)#interface ethernet 1/17                               4-119
Console(config-if)#lacp                                           4-139
Console(config-if)#exit
Console(config)#interface ethernet 1/18
Console(config-if)#lacp
Console(config-if)#end
Console#show interfaces status port-channel 1                      4-128
Information of Trunk 1
Basic information:
  Port type: 100tx
  Mac address: 22-22-22-22-22-2d
Configuration:
  Name:
  Port admin status: Up
  Speed-duplex: Auto
  Capabilities: 10half, 10full, 100half, 100full,
  Flow control status: Disabled
Current status:
  Created by: LACP
  Link status: Up
  Port operation status: Up
  Operation speed-duplex: 100full
  Flow control type: None
  Member Ports: Eth1/17, Eth1/18,
Console#

```

Statically Configuring a Trunk

Command Usage

- When configuring static trunks, you may not be able to link switches of different types, depending on the manufacturer's implementation. However, note that the static trunks on this switch are Cisco EtherChannel compatible.
- To avoid creating a loop in the network, be sure you add a static trunk via the configuration interface before connecting the ports, and also disconnect the ports before removing a static trunk via the configuration interface.



Web – Click Trunk, Trunk Configuration. Enter a trunk ID of 1-6 in the Trunk field, select any of the switch ports from the scroll-down port list, and click Add. After you have completed adding ports to the member list, click Apply.

CLI – This example creates trunk 2 with ports 11 and 12. Just connect these ports to two static trunk ports on another switch to form a trunk.

```

Console(config)#interface port-channel 2                                4-119
Console(config-if)#exit
Console(config)#interface ethernet 1/11                                4-119
Console(config-if)#channel-group 1                                     4-138
Console(config-if)#exit
Console(config)#interface ethernet 1/12
Console(config-if)#channel-group 1
Console(config-if)#end
Console#show interfaces status port-channel 1                          4-128
Information of Trunk 1
Basic information:
  Port type: 100tx
  Mac address: 22-22-22-22-22-2c
Configuration:
  Name:
  Port admin status: Up
  Speed-duplex: Auto
  Capabilities: 10half, 10full, 100half, 100full,
  Flow control status: Disabled
Current status:
  Created by: User
  Link status: Up
  Port operation status: Up
  Operation speed-duplex: 100full
  Flow control type: None
  Member Ports: Eth1/11, Eth1/12,
Console#

```

Address Table Settings

Switches store the addresses for all known devices. This information is used to pass traffic directly between the inbound and outbound ports. All the addresses learned by monitoring traffic are stored in the dynamic address table. You can also manually configure static addresses that are bound to a specific port.

Setting Static Addresses

A static address can be assigned to a specific interface on this switch. Static addresses are bound to the assigned interface and will not be moved. When a static address is seen on another interface, the address will be ignored and will not be written to the address table.

Command Attributes

- **Static Address Counts*** – The number of manually configured addresses.
- **Current Static Address Table** – Lists all the static addresses.
- **Interface** – Port or trunk associated with the device assigned a static address.
- **MAC Address** – Physical address of a device mapped to this interface.
- **VLAN** – ID of configured VLAN (1-4094).

* Web Only

Web – Click Address Table, Static Addresses. Specify the interface, the MAC address and VLAN, then click Add Static Address.

Static Addresses

Static Address Counts	<input type="text" value="1"/>	
Current Static Address Table	00-E0-29-94-34-DE, VLAN 1, Unit 1, Port 1, Permanent	
Interface	<input checked="" type="radio"/> Port <input type="text" value="1"/>	<input type="radio"/> Trunk <input type="text" value=""/>
MAC Address	<input type="text" value=""/>	<input type="text" value=""/>
VLAN	<input type="text" value="1"/>	<input type="text" value=""/>

CLI – This example adds an address to the static address table, but sets it to be deleted when the switch is reset.

```

Console(config)#mac-address-table static 00-e0-29-94-34-de
interface ethernet 1/1 vlan 1 delete-on-reset
Console(config)#
  
```

4-141

Displaying the Address Table

The Dynamic Address Table contains the MAC addresses learned by monitoring the source address for traffic entering the switch. When the destination address for inbound traffic is found in the database, the packets intended for that address are forwarded directly to the associated port. Otherwise, the traffic is flooded to all ports.

Command Usage

- **Interface** – Indicates a port or trunk.
- **MAC Address** – Physical address associated with this interface.
- **VLAN** – ID of configured VLAN (1-4094).

- **Address Table Sort Key** – You can sort the information displayed based on interface (port or trunk) or MAC address.

Web – Click Address Table, Dynamic Addresses. Specify the search type (i.e., mark the Interface, MAC Address, or VLAN checkbox), select the method of sorting the displayed addresses, and then click Query.

Dynamic Addresses

Query by:

☒ Interface ☐ Port ☐ Trunk

☐ MAC Address

☐ VLAN

Address Table Sort Key: Address

Dynamic Address Table	
Dynamic Address Counts	1
Current Dynamic Address Table	00-20-9C-23-CD-60, VLAN 2, Unit 1, Port 1, Dynamic

CLI – This example also displays the address table entries for port 1.

```

Console#show mac-address-table interface ethernet 1/1
Interface Mac Address      Vlan Type
-----
Eth 1/ 1  00-E0-29-94-34-DE  1 Permanent
Eth 1/ 1  00-20-9C-23-CD-60    2 Learned
Console#
  
```


Changing the Aging Time

You can set the aging time for entries in the dynamic address table.

Command Attributes

- **Aging Time** – The time after which a learned entry is discarded.
(Range: 10-1000000 seconds; Default: 300 seconds)

Web – Click Address Table, Address Aging. Specify the new aging time, click Apply.



CLI – This example sets the aging time to 400 seconds.

```
Console(config)#mac-address-table aging-time 400
Console(config)#
```

4-144

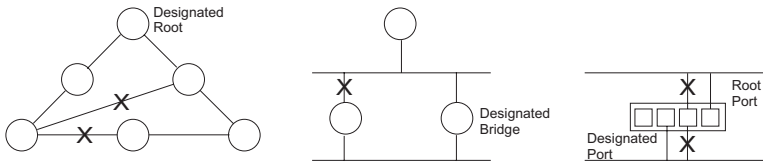
Spanning Tree Algorithm Configuration

The Spanning Tree Algorithm (STA) can be used to detect and disable network loops, and to provide backup links between switches, bridges or routers. This allows the switch to interact with other bridging devices (that is, an STA-compliant switch, bridge or router) in your network to ensure that only one route exists between any two stations on the network, and provide backup links which automatically take over when a primary link goes down.

The spanning tree algorithms supported by this switch include these versions:

- STP – Spanning Tree Protocol (IEEE 802.1D)
- RSTP – Rapid Spanning Tree Protocol (IEEE 802.1w)

STA uses a distributed algorithm to select a bridging device (STA-compliant switch, bridge or router) that serves as the root of the spanning tree network. It selects a root port on each bridging device (except for the root device) which incurs the lowest path cost when forwarding a packet from that device to the root device. It selects a designated bridging device from each LAN which incurs the lowest path cost when forwarding a packet from that LAN to the root device. It then selects a port on the designated bridging device to communicate with each attached LAN or host device as a designated port. After determining the lowest cost spanning tree, it enables all root ports and designated ports, and disables all other ports. Network packets are therefore only forwarded between root ports and designated ports, eliminating any possible network loops.



Once a stable network topology has been established, all bridges listen for Hello BPDUs (Bridge Protocol Data Units) transmitted from the Root Bridge. If a bridge does not get a Hello BPDU after a predefined interval (Maximum Age), the bridge assumes that the link to the Root Bridge is down. This bridge will then initiate negotiations with other bridges to reconfigure the network to reestablish a valid network topology.

RSTP is designed as a general replacement for the slower, legacy STP. RSTP achieves much faster reconfiguration (i.e., around one tenth of the time required by STP) by reducing the number of state changes before active ports start learning, predefining an alternate route that can be used when a node or port fails, and retaining the forwarding database for ports insensitive to changes in the tree structure when reconfiguration occurs.

Displaying Global Settings

You can display a summary of the current bridge STA information that applies to the entire switch using the STA Information screen.

Field Attributes

- **Spanning Tree State** – Shows if the switch is enabled to participate in an STA-compliant network.
- **Bridge ID** – A unique identifier for this bridge, consisting of the bridge priority and MAC address (where the address is taken from the switch system).
- **Max Age** – The maximum time (in seconds) a device can wait without receiving a configuration message before attempting to reconfigure. All device ports (except for designated ports) should receive configuration messages at regular intervals. Any port that ages out STA information (provided in the last configuration message) becomes the designated port for the attached LAN. If it is a root port, a new root port is selected from among the device ports attached to the network. (References to “ports” in this section mean “interfaces,” which includes both ports and trunks.)
- **Hello Time** – Interval (in seconds) at which the root device transmits a configuration message.
- **Forward Delay** – The maximum time (in seconds) the root device will wait before changing states (i.e., discarding to learning to forwarding). This delay is required because every device must receive information about topology changes before it starts to forward frames. In addition, each port needs time to listen for conflicting information that would make it return to a discarding state; otherwise, temporary data loops might result.
- **Designated Root** – The priority and MAC address of the device in the Spanning Tree that this switch has accepted as the root device.
 - **Root Port** – The number of the port on this switch that is closest to the root. This switch communicates with the root device through this port. If there is no root port, then this switch has been accepted as the root device of the Spanning Tree network.

- **Root Path Cost** – The path cost from the root port on this switch to the root device.
- **Configuration Changes** – The number of times the Spanning Tree has been reconfigured.
- **Last Topology Change** – Time since the Spanning Tree was last reconfigured.

These additional parameters are only displayed for the CLI:

- **Spanning tree mode** – Specifies the type of spanning tree used on this switch:
 - **STP**: Spanning Tree Protocol (IEEE 802.1D)
 - **RSTP**: Rapid Spanning Tree (IEEE 802.1w)
- **Priority** – Bridge priority is used in selecting the root device, root port, and designated port. The device with the highest priority becomes the STA root device. However, if all devices have the same priority, the device with the lowest MAC address will then become the root device.
- **Root Hello Time** – Interval (in seconds) at which this device transmits a configuration message.
- **Root Maximum Age** – The maximum time (in seconds) this device can wait without receiving a configuration message before attempting to reconfigure. All device ports (except for designated ports) should receive configuration messages at regular intervals. If the root port ages out STA information (provided in the last configuration message), a new root port is selected from among the device ports attached to the network. (References to “ports” in this section means “interfaces,” which includes both ports and trunks.)
- **Root Forward Delay** – The maximum time (in seconds) this device will wait before changing states (i.e., discarding to learning to forwarding). This delay is required because every device must receive information about topology changes before it starts to forward frames. In addition, each port needs time to listen for conflicting information that would make it return to a discarding state; otherwise, temporary data loops might result.

- **Root Hold Time** – The interval (in seconds) during which no more than two bridge configuration protocol data units shall be transmitted by this node.

Web – Click Spanning Tree, STA Information.

STA Information			
Spanning Tree:			
Spanning Tree State	Enabled	Designated Root	32768.0000ABCD0000
Bridge ID	32768.0000ABCD0000	Root Port	0
Max Age	20	Root Path Cost	0
Hello Time	2	Configuration Changes	2
Forward Delay	15	Last Topology Change	0 d 0 h 0 min 35 s

CLI – This command displays global STA settings, followed by settings for each port.

Console#show spanning-tree	4-160
Bridge-group information	

Spanning tree mode	:RSTP
Spanning tree enable/disable	:enable
Priority	:32768
Bridge Hello Time (sec.)	:2
Bridge Max Age (sec.)	:20
Bridge Forward Delay (sec.)	:15
Root Hello Time (sec.)	:2
Root Max Age (sec.)	:20
Root Forward Delay (sec.)	:15
Designated Root	:32768.0000ABCD0000
Current root port	:0
Current root cost	:0
Number of topology changes	:9
Last topology changes time (sec.)	:435571
Transmission limit	:3
Path Cost Method	:long
:	
:	

Note: The current root port and current root cost display as zero when this device is not connected to the network.

Configuring Global Settings

Global settings apply to the entire switch.

Command Usage

- **Spanning Tree Protocol**

Uses RSTP for the internal state machine, but sends only 802.1D BPDUs.

- **Rapid Spanning Tree Protocol**

RSTP supports connections to either STP or RSTP nodes by monitoring the incoming protocol messages and dynamically adjusting the type of protocol messages the RSTP node transmits, as described below:

- **STP Mode** – If the switch receives an 802.1D BPDU (i.e., STP BPDU) after a port's migration delay timer expires, the switch assumes it is connected to an 802.1D bridge and starts using only 802.1D BPDUs.
- **RSTP Mode** – If RSTP is using 802.1D BPDUs on a port and receives an RSTP BPDU after the migration delay expires, RSTP restarts the migration delay timer and begins using RSTP BPDUs on that port.

Command Attributes

Basic Configuration of Global Settings

- **Spanning Tree State** – Enables/disables STA on this switch. (Default: Enabled)
- **Spanning Tree Type** – Specifies the type of spanning tree used on this switch:
 - **STP**: Spanning Tree Protocol (IEEE 802.1D); i.e., when this option is selected, the switch will use RSTP set to STP forced compatibility mode).
 - **RSTP**: Rapid Spanning Tree (IEEE 802.1w); RSTP is the default.
- **Priority** – Bridge priority is used in selecting the root device, root port, and designated port. The device with the highest priority becomes the STA root device. However, if all devices have the same priority, the

device with the lowest MAC address will then become the root device.
(Note that lower numeric values indicate higher priority.)

Default: 32768

Range: 0-61440, in steps of 4096

Options: 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768,
36864, 40960, 45056, 49152, 53248, 57344, 61440

Root Device Configuration

- **Hello Time** – Interval (in seconds) at which the root device transmits a configuration message.

Default: 2

Minimum: 1

Maximum: The lower of 10 or $[(\text{Max. Message Age} / 2) - 1]$

- **Maximum Age** – The maximum time (in seconds) a device can wait without receiving a configuration message before attempting to reconfigure. All device ports (except for designated ports) should receive configuration messages at regular intervals. Any port that ages out STA information (provided in the last configuration message) becomes the designated port for the attached LAN. If it is a root port, a new root port is selected from among the device ports attached to the network. (References to “ports” in this section mean “interfaces,” which includes both ports and trunks.)

Default: 20

Minimum: The higher of 6 or $[2 \times (\text{Hello Time} + 1)]$.

Maximum: The lower of 40 or $[2 \times (\text{Forward Delay} - 1)]$

- **Forward Delay** – The maximum time (in seconds) this device will wait before changing states (i.e., discarding to learning to forwarding). This delay is required because every device must receive information about topology changes before it starts to forward frames. In addition, each port needs time to listen for conflicting information that would make it return to a discarding state; otherwise, temporary data loops might result.

Default: 15

Minimum: The higher of 4 or $[(\text{Max. Message Age} / 2) + 1]$

Maximum: 30

Advanced Configuration Settings for RSTP

- **Path Cost Method** – The path cost is used to determine the best path between devices. The path cost method is used to determine the range of values that can be assigned to each interface.

Long: Specifies 32-bit based values that range from 1-200,000,000.

Short: Specifies 16-bit based values that range from 1-65535. (This is the default.)

- **Transmission Limit** – The maximum transmission rate for BPDUs is specified by setting the minimum interval between the transmission of consecutive protocol messages. (Range: 1-10; Default: 3)

Web – Click Spanning Tree, STA Configuration. Modify the required attributes, and click Apply.

STA Configuration

Switch:

Spanning Tree State	Enabled
Spanning Tree Type	<input type="radio"/> STP <input checked="" type="radio"/> RSTP
Priority (0-61440)	32768

When the Switch Becomes Root:

Input Format: $2 * (\text{hello time} + 1) \leq \text{max age} \leq 2 * (\text{forward delay} - 1)$

Hello Time (1-10)	2	seconds
Maximum Age (6-40)	20	seconds
Forward Delay (4-30)	15	seconds

Advanced:

Path Cost Method	<input type="radio"/> Short <input checked="" type="radio"/> Long
Transmission Limit (1-10)	3

CLI – This example enables Spanning Tree Protocol, and then sets the indicated attributes.

Console(config)#spanning-tree	4-147
Console(config)#spanning-tree mode rst	4-148
Console(config)#spanning-tree priority 40000	4-151
Console(config)#spanning-tree hello-time 5	4-150
Console(config)#spanning-tree max-age 38	4-150
Console(config)#spanning-tree forward-time 20	4-149
Console(config)#spanning-tree pathcost method long	4-152
Console(config)#spanning-tree transmission-limit 4	4-153
Console(config)#	

Displaying Interface Settings

The STA Port Information and STA Trunk Information pages display the current status of ports and trunks in the Spanning Tree.

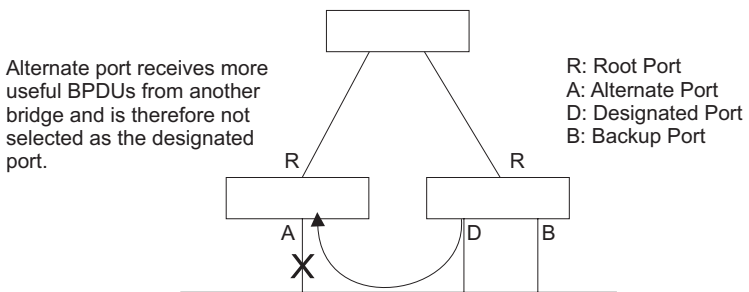
Field Attributes

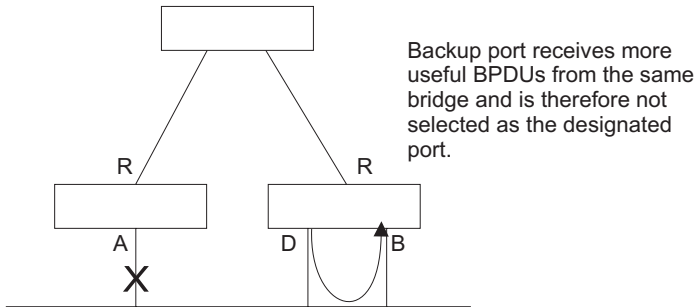
- **STA Status** – Displays current state of this port within the Spanning Tree:
 - **Discarding** - Port receives STA configuration messages, but does not forward packets.
 - **Learning** - Port has transmitted configuration messages for an interval set by the Forward Delay parameter without receiving contradictory information. Port address table is cleared, and the port begins learning addresses.
 - **Forwarding** - Port forwards packets, and continues learning addresses.

The rules defining port status are:

- A port on a network segment with no other STA compliant bridging device is always forwarding.
 - If two ports of a switch are connected to the same segment and there is no other STA device attached to this segment, the port with the smaller ID forwards packets and the other is discarding.
 - All ports are discarding when the switch is booted, then some of them change state to learning, and then to forwarding.
- **Forward Transitions** – The number of times this port has transitioned from the Learning state to the Forwarding state.

- **Designated Cost** – The cost for a packet to travel from this port to the root in the current Spanning Tree configuration. The slower the media, the higher the cost.
- **Designated Bridge** – The bridge priority and MAC address of the device through which this port must communicate to reach the root of the Spanning Tree.
- **Designated Port** – The port priority and number of the port through which this switch, acting as a designated bridge, communicates with the attached LAN or host device.
- **Oper Link Type** – The operational point-to-point status of the LAN segment attached to this interface. This parameter is determined by manual configuration or by auto-detection, as described for Admin Link Type in STA Port Configuration on page 3-99.
- **Oper Edge Port** – This parameter is initialized to the setting for Admin Edge Port in STA Port Configuration on page 3-99 (i.e., true or false), but will be set to false if a BPDU is received, indicating that another bridge is attached to this port.
- **Port Role** – Roles are assigned according to whether the port is part of the active topology connecting the bridge to the root bridge (i.e., **root** port), connecting a LAN through the bridge to the root bridge (i.e., **designated** port); or is an **alternate** or **backup** port that may provide connectivity if other bridges, bridge ports, or LANs fail or are removed. The role is set to disabled (i.e., **disabled** port) if a port has no role within the spanning tree.





- **Trunk Member** – Indicates if a port is a member of a trunk.
(STA Port Information only)

These additional parameters are only displayed for the CLI:

- **Admin status** – Shows if STA has been enabled on this interface.
- **Path Cost** – This parameter is used by the STA to determine the best path between devices. Therefore, lower values should be assigned to ports attached to faster media, and higher values assigned to ports with slower media. (Path cost takes precedence over port priority.)
- **Priority** – Defines the priority used for this port in the Spanning Tree Algorithm. If the path cost for all ports on a switch is the same, the port with the highest priority (i.e., lowest value) will be configured as an active link in the Spanning Tree. This makes a port with higher priority less likely to be blocked if the Spanning Tree Algorithm is detecting network loops. Where more than one port is assigned the highest priority, the port with the lowest numeric identifier will be enabled.
- **Designated root** – The priority and MAC address of the device in the Spanning Tree that this switch has accepted as the root device.
- **Fast forwarding** – This field provides the same information as Admin Edge port, and is only included for backward compatibility with earlier products.
- **Admin Edge Port** – You can enable this option if an interface is attached to a LAN segment that is at the end of a bridged LAN or to an end node. Since end nodes **cannot** cause forwarding loops, they can pass

directly through to the spanning tree forwarding state. Specifying Edge Ports provides quicker convergence for devices such as workstations or servers, retains the current forwarding database to reduce the amount of frame flooding required to rebuild address tables during reconfiguration events, does not cause the spanning tree to reconfigure when the interface changes state, and also overcomes other STA-related timeout problems. However, remember that Edge Port should only be enabled for ports connected to an end-node device.

- **Admin Link Type** – The link type attached to this interface.
 - Point-to-Point – A connection to exactly one other bridge.
 - Shared – A connection to two or more bridges.
 - Auto – The switch automatically determines if the interface is attached to a point-to-point link or to shared media.

Web – Click Spanning Tree, STA Port Information or STA Trunk Information.

STA Port Information									
Port	STA Status	Forward Transitions	Designated Cost	Designated Bridge	Designated Port	Oper Link Type	Oper Edge Port	Port Role	Trunk Member
1	Forwarding	1	0	32768.0000ABCD0000	128.1	Point-to-Point	Disabled	Designated	
2	Discarding	0	0	32768.0000ABCD0000	128.2	Point-to-Point	Disabled	Disabled	
3	Discarding	0	0	32768.0000ABCD0000	128.3	Point-to-Point	Disabled	Disabled	
4	Discarding	0	0	32768.0000ABCD0000	128.4	Point-to-Point	Disabled	Disabled	
5	Discarding	0	0	32768.0000ABCD0000	128.5	Point-to-Point	Disabled	Disabled	
6	Discarding	0	0	32768.0000ABCD0000	128.6	Point-to-Point	Disabled	Disabled	
7	Forwarding	1	0	32768.0000ABCD0000	128.7	Point-to-Point	Disabled	Designated	

CLI – This example shows the STA attributes for port 5.

```

Console#show spanning-tree ethernet 1/5
Eth 1/ 1 information
-----
Admin status      : enable
Role              : designate
State             : forwarding
Path cost         : 100000
Priority           : 128
Designated cost   : 0
Designated port   : 128.1
Designated root   : 32768.0000ABCD0000
Designated bridge : 32768.0000ABCD0000
Forward transitions : 2
Fast forwarding   : disable
Admin edge port   : disable
Oper edge port    : disable
Admin Link type   : auto
Oper Link type    : point-to-point

Console#
  
```

Configuring Interface Settings

You can configure RSTP attributes for specific interfaces, including port priority, path cost, link type, and edge port. You may use a different priority or path cost for ports of the same media type to indicate the preferred path, link type to indicate a point-to-point connection or shared-media connection, and edge port to indicate if the attached device can support fast forwarding.

Command Attributes

The following attributes are read-only and cannot be changed:

- **STA State** – Displays current state of this port within the Spanning Tree. (See Displaying Interface Settings on page 3-95 for additional information.)
 - **Discarding** - Port receives STA configuration messages, but does not forward packets.
 - **Learning** - Port has transmitted configuration messages for an interval set by the Forward Delay parameter without receiving contradictory information. Port address table is cleared, and the port begins learning addresses.

- **Forwarding** - Port forwards packets, and continues learning addresses.
- **Trunk** – Indicates if a port is a member of a trunk.
(STA Port Configuration only)

The following interface attributes can be configured:

- **Priority** – Defines the priority used for this port in the Spanning Tree Protocol. If the path cost for all ports on a switch are the same, the port with the highest priority (i.e., lowest value) will be configured as an active link in the Spanning Tree. This makes a port with higher priority less likely to be blocked if the Spanning Tree Protocol is detecting network loops. Where more than one port is assigned the highest priority, the port with lowest numeric identifier will be enabled.

Default: 128

Range: 0-240, in steps of 16

- **Path Cost** – This parameter is used by the STP to determine the best path between devices. Therefore, lower values should be assigned to ports attached to faster media, and higher values assigned to ports with slower media. (Path cost takes precedence over port priority.) Note that when the Path Cost Method is set to short (page 3-63), the maximum path cost is 65,535.
 - Range –
 - Ethernet: 200,000-20,000,000
 - Fast Ethernet: 20,000-2,000,000
 - Gigabit Ethernet: 2,000-200,000
 - Default –
 - Ethernet – Half duplex: 2,000,000; full duplex: 1,000,000; trunk: 500,000
 - Fast Ethernet – Half duplex: 200,000; full duplex: 100,000; trunk: 50,000
 - Gigabit Ethernet – Full duplex: 10,000; trunk: 5,000

- **Admin Link Type** – The link type attached to this interface.
 - Point-to-Point – A connection to exactly one other bridge.
 - Shared – A connection to two or more bridges.
 - Auto – The switch automatically determines if the interface is attached to a point-to-point link or to shared media. (This is the default setting.)
- **Admin Edge Port** (Fast Forwarding) – You can enable this option if an interface is attached to a LAN segment that is at the end of a bridged LAN or to an end node. Since end nodes **cannot** cause forwarding loops, they can pass directly through to the spanning tree forwarding state. Specifying Edge Ports provides quicker convergence for devices such as workstations or servers, retains the current forwarding database to reduce the amount of frame flooding required to rebuild address tables during reconfiguration events, does not cause the spanning tree to initiate reconfiguration when the interface changes state, and also overcomes other STA-related timeout problems. However, remember that Edge Port should only be enabled for ports connected to an end-node device. (Default: Disabled)
- **Migration** – If at any time the switch detects STP BPDUs, including Configuration or Topology Change Notification BPDUs, it will automatically set the selected interface to forced STP-compatible mode. However, you can also use the Protocol Migration button to manually re-check the appropriate BPDU format (RSTP or STP-compatible) to send on the selected interfaces. (Default: Disabled)

Web – Click Spanning Tree, STA Port Configuration or STA Trunk Configuration. Modify the required attributes, then click Apply.

STA Port Configuration

Port	STA State	Priority (0-240)	Path Cost (1-200000000)	Admin Link Type	Admin Edge Port (Fast Forwarding)	Migration	Trunk
1	Forwarding	128	100000	Auto	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	
2	Forwarding	128	100000	Auto	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	
3	Forwarding	128	100000	Auto	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	
4	Discarding	128	100000	Auto	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	
5	Discarding	128	100000	Auto	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	
6	Discarding	128	100000	Auto	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	
7	Forwarding	0	50	Auto	<input type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled	

CLI – This example sets STA attributes for port 7.

```

Console(config)#interface ethernet 1/7                                4-119
Console(config-if)#spanning-tree port-priority 0                      4-155
Console(config-if)#spanning-tree cost 50                             4-154
Console(config-if)#spanning-tree link-type auto                      4-158
Console(config-if)#no spanning-tree edge-port                        4-156
Console(config-if)#spanning-tree protocol-migration                  4-159
Console(config-if)#

```

VLAN Configuration

Overview

In large networks, routers are used to isolate broadcast traffic for each subnet into separate domains. This switch provides a similar service at Layer 2 by using VLANs to organize any group of network nodes into separate broadcast domains. VLANs confine broadcast traffic to the originating group, and can eliminate broadcast storms in large networks. This also provides a more secure and cleaner network environment.

An IEEE 802.1Q VLAN is a group of ports that can be located anywhere in the network, but communicate as though they belong to the same physical segment.

VLANs help to simplify network management by allowing you to move devices to a new VLAN without having to change any physical connections. VLANs can be easily organized to reflect departmental groups (such as Marketing or R&D), usage groups (such as e-mail), or multicast groups (used for multimedia applications such as videoconferencing).

VLANs provide greater network efficiency by reducing broadcast traffic, and allow you to make network changes without having to update IP addresses or IP subnets. VLANs inherently provide a high level of network security since traffic must pass through a configured Layer 3 link to reach a different VLAN.

This switch supports the following VLAN features:

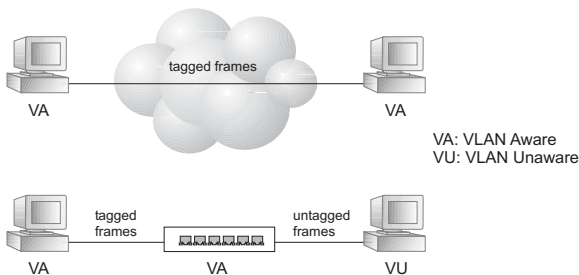
- Up to 255 VLANs based on the IEEE 802.1Q standard
- Distributed VLAN learning across multiple switches using explicit or implicit tagging and GVRP protocol
- Port overlapping, allowing a port to participate in multiple VLANs
- End stations can belong to multiple VLANs
- Passing traffic between VLAN-aware and VLAN-unaware devices
- Priority tagging

Assigning Ports to VLANs

Before enabling VLANs for the switch, you must first assign each port to the VLAN group(s) in which it will participate. By default all ports are assigned to VLAN 1 as untagged ports. Add a port as a tagged port if you want it to carry traffic for one or more VLANs, and any intermediate network devices or the host at the other end of the connection supports VLANs. Then assign ports on the other VLAN-aware network devices along the path that will carry this traffic to the same VLAN(s), either manually or dynamically using GVRP. However, if you want a port on this

switch to participate in one or more VLANs, but none of the intermediate network devices nor the host at the other end of the connection supports VLANs, then you should add this port to the VLAN as an untagged port.

Note: VLAN-tagged frames can pass through VLAN-aware or VLAN-unaware network interconnection devices, but the VLAN tags should be stripped off before passing it on to any end-node host that does not support VLAN tagging.



VLAN Classification – When the switch receives a frame, it classifies the frame in one of two ways. If the frame is untagged, the switch assigns the frame to an associated VLAN (based on the default VLAN ID of the receiving port). But if the frame is tagged, the switch uses the tagged VLAN ID to identify the port broadcast domain of the frame.

Port Overlapping – Port overlapping can be used to allow access to commonly shared network resources among different VLAN groups, such as file servers or printers. Note that if you implement VLANs which do not overlap, but still need to communicate, you can connect them by enabled routing on this switch.

Untagged VLANs – Untagged (or static) VLANs are typically used to reduce broadcast traffic and to increase security. A group of network users assigned to a VLAN form a broadcast domain that is separate from other VLANs configured on the switch. Packets are forwarded only between ports that are designated for the same VLAN. Untagged VLANs can be

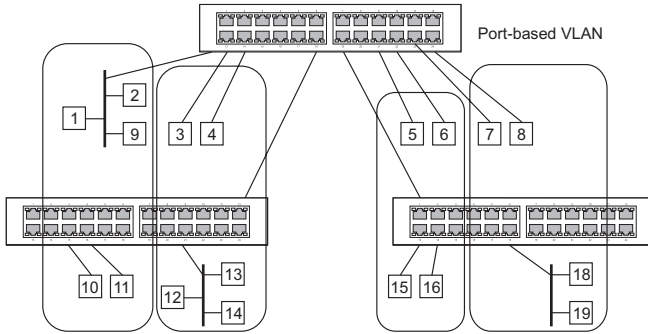
used to manually isolate user groups or subnets. However, you should use IEEE 802.3 tagged VLANs with GVRP whenever possible to fully automate VLAN registration.

Automatic VLAN Registration – GVRP (GARP VLAN Registration Protocol) defines a system whereby the switch can automatically learn the VLANs to which each end station should be assigned. If an end station (or its network adapter) supports the IEEE 802.1Q VLAN protocol, it can be configured to broadcast a message to your network indicating the VLAN groups it wants to join. When this switch receives these messages, it will automatically place the receiving port in the specified VLANs, and then forward the message to all other ports. When the message arrives at another switch that supports GVRP, it will also place the receiving port in the specified VLANs, and pass the message on to all other ports. VLAN requirements are propagated in this way throughout the network. This allows GVRP-compliant devices to be automatically configured for VLAN groups based solely on endstation requests.

To implement GVRP in a network, first add the host devices to the required VLANs (using the operating system or other application software), so that these VLANs can be propagated onto the network. For both the edge switches attached directly to these hosts, and core switches in the network, enable GVRP on the links between these devices. You should also determine security boundaries in the network and disable GVRP on the boundary ports to prevent advertisements from being propagated, or forbid those ports from joining restricted VLANs.

Note: If you have host devices that do not support GVRP, you should configure static or untagged VLANs for the switch ports connected to these devices (as described in “Adding Static Members to VLANs (VLAN Index)” on page 3-111). But you can

still enable GVRP on these edge switches, as well as on the core switches in the network.



Forwarding Tagged/Untagged Frames

If you want to create a small port-based VLAN for devices attached directly to a single switch, you can assign ports to the same untagged VLAN. However, to participate in a VLAN group that crosses several switches, you should create a VLAN for that group and enable tagging on all ports.

Ports can be assigned to multiple tagged or untagged VLANs. Each port on the switch is therefore capable of passing tagged or untagged frames. When forwarding a frame from this switch along a path that contains any VLAN-aware devices, the switch should include VLAN tags. When forwarding a frame from this switch along a path that does not contain any VLAN-aware devices (including the destination host), the switch must first strip off the VLAN tag before forwarding the frame. When the switch receives a tagged frame, it will pass this frame onto the VLAN(s) indicated by the frame tag. However, when this switch receives an untagged frame from a VLAN-unaware device, it first decides where to forward the frame, and then inserts a VLAN tag reflecting the ingress port's default VID.

Enabling or Disabling GVRP (Global Setting)

GARP VLAN Registration Protocol (GVRP) defines a way for switches to exchange VLAN information in order to register VLAN members on ports across the network. VLANs are dynamically configured based on join messages issued by host devices and propagated throughout the network. GVRP must be enabled to permit automatic VLAN registration, and to support VLANs which extend beyond the local switch.

(Default: Disabled)

Web – Click System, Bridge Extension. Enable or disable GVRP, click Apply.

Bridge Capability	
Extended Multicast Filtering Services	No
Traffic Classes	Enabled
Static Entry Individual Port	Yes
VLAN Learning	IVL
Configurable PVID Tagging	Yes
Local VLAN Capable	No

Traffic Classes	<input checked="" type="checkbox"/> Enable
GMRP	<input type="checkbox"/> Enable
GVRP	<input type="checkbox"/> Enable

CLI – This example enables GVRP for the switch.

```
Console(config)#bridge-ext gvrp
Console(config)#
```

4-175

Displaying Basic VLAN Information

The VLAN Basic Information page displays basic information on the VLAN type supported by the switch.

Field Attributes

- **VLAN Version Number*** – The VLAN version used by this switch as specified in the IEEE 802.1Q standard.
- **Maximum VLAN ID** – Maximum VLAN ID recognized by this switch.

- **Maximum Number of Supported VLANs** – Maximum number of VLANs that can be configured on this switch.

* Web Only

Web – Click VLAN, VLAN Base Information.

VLAN Basic Information	
VLAN Version Number	1
Maximum VLAN ID	4094
Maximum Number of Supported VLANs	255

CLI – Enter the following command.

<pre> Console#show bridge-ext Max support vlan numbers: 255 Max support vlan ID: 4094 Extended multicast filtering services: No Static entry individual port: Yes VLAN learning: IVL Configurable PVID tagging: Yes Local VLAN capable: No Traffic classes: Enabled Global GVRP status: Disabled GMRP: Disabled Console# </pre>	4-176
---	-------

Displaying Current VLANs

The VLAN Current Table shows the current port members of each VLAN and whether or not the port supports VLAN tagging. Ports assigned to a large VLAN group that crosses several switches should use VLAN tagging. However, if you just want to create a small port-based VLAN for one or two switches, you can disable tagging.

Command Attributes (Web)

- **VLAN ID** – ID of configured VLAN (1-4094).
- **Up Time at Creation** – Time this VLAN was created (i.e., System Up Time).

- **Status** – Shows how this VLAN was added to the switch.
 - **Dynamic GVRP**: Automatically learned via GVRP.
 - **Permanent**: Added as a static entry.
- **Egress Ports** – Shows all the VLAN port members.
- **Untagged Ports** – Shows the untagged VLAN port members.

Web – Click VLAN, VLAN Current Table. Select any ID from the scroll-down list.

VLAN Current Table

VLAN ID: 1

Up Time at Creation0 d 0 h 0 min 7 s
StatusPermanent

Egress Ports	Untagged Ports
Unit1 Port1	Unit1 Port1
Unit1 Port2	Unit1 Port2
Unit1 Port3	Unit1 Port3
Unit1 Port4	Unit1 Port4
Unit1 Port6	Unit1 Port6
Unit1 Port7	Unit1 Port7
Unit1 Port8	Unit1 Port8
Unit1 Port9	Unit1 Port9

Command Attributes (CLI)

- **VLAN** – ID of configured VLAN (1-4094, no leading zeroes).
- **Type** – Shows how this VLAN was added to the switch.
 - **Dynamic**: Automatically learned via GVRP.
 - **Static**: Added as a static entry.
- **Name** – Name of the VLAN (1 to 32 characters).
- **Status** – Shows if this VLAN is enabled or disabled.
 - **Active**: VLAN is operational.
 - **Suspend**: VLAN is suspended; i.e., does not pass packets.
- **Ports / Channel groups** – Shows the VLAN interface members.

CLI – Current VLAN information can be displayed with the following command.

Console#show vlan id 1								4-172
VLAN	Type	Name	Status	Ports/Channel groups				
1	Static	DefaultVlan	Active	Eth1/1	Eth1/2	Eth1/3	Eth1/4	Eth1/5
				Eth1/6	Eth1/7	Eth1/8	Eth1/9	Eth1/10
				Eth1/11	Eth1/12	Eth1/13	Eth1/14	Eth1/15
				Eth1/16	Eth1/17	Eth1/18	Eth1/19	Eth1/20
				Eth1/21	Eth1/22	Eth1/23	Eth1/24	Eth1/25
				Eth1/26				
Console#								

Creating VLANs

Use the VLAN Static List to create or remove VLAN groups. To propagate information about VLAN groups used on this switch to external network devices, you must specify a VLAN ID for each of these groups.

Command Attributes

- **Current** – Lists all the current VLAN groups created for this system. Up to 255 VLAN groups can be defined. VLAN 1 is the default untagged VLAN.
- **New** – Allows you to specify the name and numeric identifier for a new VLAN group. (The VLAN name is only used for management on this system; it is not added to the VLAN tag.)
- **VLAN ID** – ID of configured VLAN (1-4094, no leading zeroes).
- **VLAN Name** – Name of the VLAN (1 to 32 characters).
- **Status (Web)** – Enables or disables the specified VLAN.
 - **Enable:** VLAN is operational.
 - **Disable:** VLAN is suspended; i.e., does not pass packets.
- **State (CLI)** – Enables or disables the specified VLAN.
 - **Active:** VLAN is operational.
 - **Suspend:** VLAN is suspended; i.e., does not pass packets.
- **Add** – Adds a new VLAN group to the current list.

- **Remove** – Removes a VLAN group from the current list. If any port is assigned to this group as untagged, it will be reassigned to VLAN group 1 as untagged.

Web – Click VLAN, VLAN Static List. To create a new VLAN, enter the VLAN ID and VLAN name, mark the Enable checkbox to activate the VLAN, and then click Add.

VLAN Static List

Current:
1, DefaultVlan, Enabled

New:
 VLAN ID (1-4094): 2
 VLAN Name: R&D
 Status: ☒ Enable

Buttons: <<Add, Remove, Add

CLI – This example creates a new VLAN.

```

Console(config)#vlan database                                4-162
Console(config-vlan)#vlan 2 name R&D media ethernet state active 4-163
Console(config-vlan)#end
Console#show vlan                                           4-172
VLAN Type      Name                Status    Ports/Channel groups
-----
 1 Static      DefaultVlan        Active    Eth1/ 1 Eth1/ 2 Eth1/ 3 Eth1/ 4 Eth1/ 5
                                     Eth1/ 6 Eth1/ 7 Eth1/ 8 Eth1/ 9 Eth1/10
                                     Eth1/11 Eth1/12 Eth1/13 Eth1/14 Eth1/15
                                     Eth1/16 Eth1/17 Eth1/18 Eth1/19 Eth1/20
                                     Eth1/21 Eth1/22 Eth1/23 Eth1/24 Eth1/25
                                     Eth1/26
 2 Static      R&D                Active
Console(config-vlan)#
  
```

Adding Static Members to VLANs (VLAN Index)

Use the VLAN Static Table to configure port members for the selected VLAN index. Assign ports as tagged if they are connected to 802.1Q VLAN compliant devices, or untagged they are not connected to any VLAN-aware devices. Or configure a port as forbidden to prevent the switch from automatically adding it to a VLAN via the GVRP protocol.

Notes: 1. You can also use the VLAN Static Membership by Port page to configure VLAN groups based on the port index (page 3-113). However, note that this configuration page can only add ports to a VLAN as tagged members.

2. VLAN 1 is the default untagged VLAN containing all ports on the switch, and can only be modified by first reassigning the default port VLAN ID as described under “Configuring VLAN Behavior for Interfaces” on page 3-114.

Command Attributes

- **VLAN** – ID of configured VLAN (1-4094, no leading zeroes).
- **Name** – Name of the VLAN (1 to 32 characters).
- **Status** – Enables or disables the specified VLAN.
 - **Enable:** VLAN is operational.
 - **Disable:** VLAN is suspended; i.e., does not pass packets.
- **Port** – Port identifier.
- **Trunk** – Trunk identifier.
- **Membership Type** – Select VLAN membership for each interface by marking the appropriate radio button for a port or trunk:
 - **Tagged:** Interface is a member of the VLAN. All packets transmitted by the port will be tagged, that is, carry a tag and therefore carry VLAN or CoS information.
 - **Untagged:** Interface is a member of the VLAN. All packets transmitted by the port will be untagged, that is, not carry a tag and therefore not carry VLAN or CoS information. Note that an interface must be assigned to at least one group as an untagged port.
 - **Forbidden:** Interface is forbidden from automatically joining the VLAN via GVRP. For more information, see “Automatic VLAN Registration” on page 3-105.
 - **None:** Interface is not a member of the VLAN. Packets associated with this VLAN will not be transmitted by the interface.
- **Trunk Member** – Indicates if a port is a member of a trunk. To add a trunk to the selected VLAN, use the last table on the VLAN Static Table page.

Web – Click VLAN, VLAN Static Table. Select a VLAN ID from the scroll-down list. Modify the VLAN name and status if required. Select the membership type by marking the appropriate radio button in the list of ports or trunks. Click Apply.

VLAN Static Table

VLAN:

Name:

Status: ☒ Enable

Port	Tagged	Untagged	Forbidden	None	Trunk Member
1	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	
2	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	
3	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	
4	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	
5	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	

CLI – The following example adds tagged and untagged ports to VLAN 2.

```

Console(config)#interface ethernet 1/1                                4-119
Console(config-if)#switchport allowed vlan add 2 tagged              4-170
Console(config-if)#exit
Console(config)#interface ethernet 1/2
Console(config-if)#switchport allowed vlan add 2 untagged
Console(config-if)#exit
Console(config)#interface ethernet 1/13
Console(config-if)#switchport allowed vlan add 2 tagged
  
```

Adding Static Members to VLANs (Port Index)

Use the VLAN Static Membership by Port menu to assign VLAN groups to the selected interface as a tagged member.

Command Attributes

- **Interface** – Port or trunk identifier.
- **Member** – VLANs for which the selected interface is a tagged member.
- **Non-Member** – VLANs for which the selected interface is not a tagged member.

Web – Open VLAN, VLAN Static Membership. Select an interface from the scroll-down box (Port or Trunk). Click Query to display membership information for the interface. Select a VLAN ID, and then click Add to add the interface as a tagged member, or click Remove to remove the interface. After configuring VLAN membership for each interface, click Apply.

VLAN Static Membership by Port

Interface: ☒ Port 3 ☐ Trunk

Query

Member: Vlan 1

Non-Member: Vlan 2

<< Add

Remove >>

CLI – This example adds Port 3 to VLAN 1 as a tagged port, and removes Port 3 from VLAN 2.

```
Console(config)#interface ethernet 1/3          4-119
Console(config-if)#switchport allowed vlan add 1 tagged 4-170
Console(config-if)#switchport allowed vlan remove 2
```

Configuring VLAN Behavior for Interfaces

You can configure VLAN behavior for specific interfaces, including the default VLAN identifier (PVID), accepted frame types, ingress filtering, GVRP status, and GARP timers.

Command Usage

- **GVRP** – GARP VLAN Registration Protocol defines a way for switches to exchange VLAN information in order to automatically register VLAN members on interfaces across the network.
- **GARP** – Group Address Registration Protocol is used by GVRP to register or deregister client attributes for client services within a bridged LAN. The default values for the GARP timers are independent of the

media access method or data rate. These values should not be changed unless you are experiencing difficulties with GVRP registration/deregistration.

Command Attributes

- **PVID** – VLAN ID assigned to untagged frames received on the interface. (Default: 1)
 - If an interface is not a member of VLAN 1 and you assign its PVID to this VLAN, the interface will automatically be added to VLAN 1 as an untagged member. For all other VLANs, an interface must first be configured as an untagged member before you can assign its PVID to that group.
- **Acceptable Frame Type** – Sets the interface to accept all frame types, including tagged or untagged frames, or only tagged frames. When set to receive all frame types, any received frames that are untagged are assigned to the default VLAN. (Option: All, Tagged; Default: All)
- **Ingress Filtering** – Determines how to process frames tagged for VLANs for which the ingress port is not a member. (Default: Disabled)
 - Ingress filtering only affects tagged frames.
 - If ingress filtering is disabled and a port receives frames tagged for VLANs for which it is not a member, these frames will be flooded to all other ports (except for those VLANs explicitly forbidden on this port).
 - If ingress filtering is enabled and a port receives frames tagged for VLANs for which it is not a member, these frames will be discarded.
 - Ingress filtering does not affect VLAN independent BPDU frames, such as GVRP or STP. However, they do affect VLAN dependent BPDU frames, such as GMRP.
- **GVRP Status** – Enables/disables GVRP for the interface. GVRP must be globally enabled for the switch before this setting can take effect. (See “Displaying Bridge Extension Capabilities” on page 3-16.) When disabled, any GVRP packets received on this port will be discarded and no GVRP registrations will be propagated from other ports. (Default: Disabled)

- **GARP Join Timer*** – The interval between transmitting requests/queries to participate in a VLAN group. (Range: 20-1000 centiseconds; Default: 20)
- **GARP Leave Timer*** – The interval a port waits before leaving a VLAN group. This time should be set to more than twice the join time. This ensures that after a Leave or LeaveAll message has been issued, the applicants can rejoin before the port actually leaves the group. (Range: 60-3000 centiseconds; Default: 60)
- **GARP LeaveAll Timer*** – The interval between sending out a LeaveAll query message for VLAN group participants and the port leaving the group. This interval should be considerably larger than the Leave Time to minimize the amount of traffic generated by nodes rejoining the group. (Range: 500-18000 centiseconds; Default: 1000)
- **Trunk Member** – Indicates if a port is a member of a trunk. To add a trunk to the selected VLAN, use the last table on the VLAN Static Table page.
- **Mode** – Indicates VLAN membership mode for an interface. (Default: 1Q Trunk)
 - **1Q Trunk** – Specifies a port as an end-point for a VLAN trunk. A trunk is a direct link between two switches, so the port transmits tagged frames that identify the source VLAN. However, note that frames belonging to the port's default VLAN (i.e., associated with the PVID) are sent untagged.
 - **Hybrid** – Specifies a hybrid VLAN interface. The port may transmit tagged or untagged frames.

* Timer settings must follow this rule: 2 x (join timer) < leave timer < leaveAll timer

Web – Click VLAN, VLAN Port Configuration or VLAN Trunk Configuration. Fill in the required settings for each interface, click Apply.

VLAN Port Configuration									
Port	PVID	Acceptable Frame Type	Ingress Filtering	GVRP Status	GARP Join Timer (Centi Seconds) (20-1000)	GARP Leave Timer (Centi Seconds) (60-3000)	GARP LeaveAll Timer (Centi Seconds) (500-18000)	Trunk Member	Mode
1	1	ALL	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	20	60	1000		Hybrid
2	1	ALL	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	20	60	1000		Hybrid
3	3	Tagged	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	20	60	1000		Hybrid
4	1	ALL	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	20	60	1000		Hybrid
5	1	ALL	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled	30	90	2000		Hybrid
6	1	ALL	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	20	60	1000		Hybrid

CLI – This example sets port 3 to accept only tagged frames, assigns PVID 3 as the native VLAN ID, enables GVRP, sets the GARP timers, and then sets the switchport mode to hybrid.

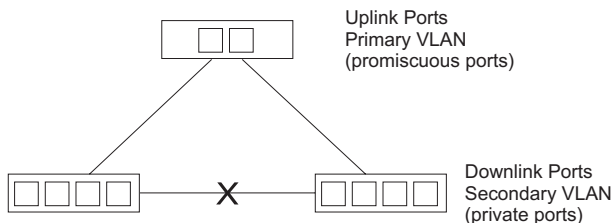
```

Console(config)#interface ethernet 1/3                               4-119
Console(config-if)#switchport acceptable-frame-types tagged         4-167
Console(config-if)#switchport ingress-filtering                     4-168
Console(config-if)#switchport native vlan 3                         4-169
Console(config-if)#switchport gvrp                                  4-177
Console(config-if)#garp timer join 10                               4-178
Console(config-if)#garp timer leave 90
Console(config-if)#garp timer leaveall 2000
Console(config-if)#switchport mode hybrid                           4-166
Console(config-if)#

```

Configuring Private VLANs

Private VLANs provide port-based security and isolation between ports within the assigned VLAN. Data traffic on downlink ports can only be forwarded to, and from, uplink ports. (Note that private VLANs and normal VLANs can exist simultaneously within the same switch.)



Enabling Private VLANs

Use the Private VLAN Status page to enable/disable the Private VLAN function.

Web – Click Private VLAN, Private VLAN Status. Select Enable or Disable from the scroll-down box, and click Apply.

Private VLAN Status

Private VLAN Status Enabled

CLI – This example enables private VLANs.

```
Console(config)#pvlan
Console(config)#
```

4-173

Configuring Uplink and Downlink Ports

Use the Private VLAN Link Status page to set ports as downlink or uplink ports. Ports designated as downlink ports can not communicate with any other ports on the switch except for the uplink ports. Uplink ports can communicate with any other ports on the switch and with any designated downlink ports.

Web – Click Private VLAN, Private VLAN Link Status. Mark the ports that will serve as uplinks and downlinks for the private VLAN, then click Apply.

Private VLAN Link Status

Port	Uplink	Downlink	None	Trunk Member
1	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	
2	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	
3	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	
4	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	
5	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	
6	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	
7	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	

CLI – This configures ports 3 and 4 as uplinks and ports 5 and 6 as downlinks.

```
Console(config)#pvlan uplink 1/3-4 downlink 1/5-6
Console(config)#
```

4-173

Class of Service Configuration

Class of Service (CoS) allows you to specify which data packets have greater precedence when traffic is buffered in the switch due to congestion. This switch supports CoS with four priority queues for each port. Data packets in a port's high-priority queue will be transmitted before those in the lower-priority queues. You can set the default priority for each interface, and configure the mapping of frame priority tags to the switch's priority queues.

Setting the Default Priority for Interfaces

You can specify the default port priority for each interface on the switch. All untagged packets entering the switch are tagged with the specified default port priority, and then sorted into the appropriate priority queue at the output port.

Command Usage

- This switch provides four priority queues for each port. It uses Weighted Round Robin to prevent head-of-queue blockage.
- The default priority applies for an untagged frame received on a port set to accept all frame types (i.e., receives both untagged and tagged frames). This priority does not apply to IEEE 802.1Q VLAN tagged frames. If the incoming frame is an IEEE 802.1Q VLAN tagged frame, the IEEE 802.1p User Priority bits will be used.
- If the output port is an untagged member of the associated VLAN, these frames are stripped of all VLAN tags prior to transmission.

Command Attributes

- **Default Priority*** – The priority that is assigned to untagged frames received on the specified interface. (Range: 0 - 7, Default: 0)
- **Number of Egress Traffic Classes** – The number of queue buffers provided for each port.

* CLI displays this information as "Priority for untagged traffic."

Web – Click Priority, Default Port Priority or Default Trunk Priority. Modify the default priority for any interface, then click Apply.

Port Priority Configuration			
Port	Default Priority	Number of Egress Traffic Classes	Trunk
1	0 (0-7)	4	
2	0 (0-7)	4	
3	5 (0-7)	4	
4	0 (0-7)	4	
5	0 (0-7)	4	

CLI – This example assigns a default priority of 5 to port 3.

```

Console(config)#interface ethernet 1/3          4-119
Console(config-if)#switchport priority default 5  4-182
Console(config-if)#end
Console#show interfaces switchport ethernet 1/5  4-131
Information of Eth 1/5
Broadcast threshold: Enabled, 500 packets/second
Lacp status: Disabled
VLAN membership mode: Hybrid
Ingress rule: Disabled
Acceptable frame type: All frames
Native VLAN: 1
Priority for untagged traffic: 5
Gvrp status: Disabled
Allowed Vlan: 1(u),
Forbidden Vlan:
Console#

```

Mapping CoS Values to Egress Queues

This switch processes Class of Service (CoS) priority tagged traffic by using four priority queues for each port, with service schedules based on Weighted Round Robin (WRR). Up to eight separate traffic priorities are defined in IEEE 802.1p. The default priority levels are assigned according to recommendations in the IEEE 802.1p standard as shown in the following table.

	Queue			
	0	1	2	3
Priority		0		
	1			
	2			
		3		
			4	
			5	
				6
				7

The priority levels recommended in the IEEE 802.1p standard for various network applications are shown in the following table. However, you can map the priority levels to the switch’s output queues in any way that benefits application traffic for your own network.

Priority Level	Traffic Type
1	Background
2	(Spare)
0 (default)	Best Effort
3	Excellent Effort
4	Controlled Load
5	Video, less than 100 milliseconds latency and jitter
6	Voice, less than 10 milliseconds latency and jitter
7	Network Control

Command Attributes

- **Priority** – CoS value. (Range: 0-7, where 7 is the highest priority)
- **Traffic Class*** – Output queue buffer. (Range: 0-3, where 3 is the highest CoS priority queue)

* CLI shows Queue ID.

Web – Click Priority, Traffic Classes. Mark an interface and click Select to display the current mapping of CoS values to output queues. Assign priorities to the traffic classes (i.e., output queues) for the selected interface, then click Apply.

Traffic Classes

Interface

☒ Port

1

☐ Trunk

Select

Priority	Traffic Class
0	<div>0</div> (0-3)
1	<div>0</div> (0-3)
2	<div>0</div> (0-3)
3	<div>1</div> (0-3)
4	<div>2</div> (0-3)
5	<div>2</div> (0-3)
6	<div>3</div> (0-3)
7	<div>3</div> (0-3)

CLI – The following example shows how to map CoS values 0, 1 and 2 to priority queue 0, value 3 to priority queue 1, values 4 and 5 to priority queue 2, and values 6 and 7 to priority queue 3.

```

Console(config)#interface ethernet 1/1                                4-119
Console(config)#queue cos-map 0 0 1 2                               4-184
Console(config)#queue cos-map 1 3
Console(config)#queue cos-map 2 4 5
Console(config)#queue cos-map 3 6 7
Console(config)#exit
Console#show queue cos-map ethernet 1/1                             4-186
Information of Eth 1/1
  Queue ID Traffic class
  -----
      0      0 1 2
      1      3
      2      4 5
      3      6 7
Console#

```

- * Mapping specific values for CoS priorities is implemented as an interface configuration command, but any changes will apply to the all interfaces on the switch.

Setting the Service Weight for Traffic Classes

This switch uses the Weighted Round Robin (WRR) algorithm to determine the frequency at which it services each priority queue. As described in “Mapping CoS Values to Egress Queues” on page 3-122, the traffic classes are mapped to one of the four egress queues provided for each port. You can assign a weight to each of these queues (and thereby to the corresponding traffic priorities). This weight sets the frequency at which each queue will be polled for service, and subsequently affects the response time for software applications assigned a specific priority value.

Command Attributes

- **WRR Setting Table*** – Displays a list of weights for each traffic class (i.e., queue).
- **Weight Value** – Set a new weight for the selected traffic class. (Range: 1-255)

- * CLI shows Queue ID.

Web – Click Priority, Queue Scheduling. Select a traffic class (i.e., output queue), enter a weight, then click Apply.

Queue Scheduling

WRR Setting Table

Traffic Class 0 - weight 1
Traffic Class 1 - weight 4
Traffic Class 2 - weight 16
Traffic Class 3 - weight 64

Weight Value (1-255)

CLI – The following example shows how to assign WRR weights of 16, 64, 128 and 240 to the CoS priority queues 0, 1, 2 and 3.

```

Console(config)#queue bandwidth 16 64 128 240          4-183
Console(config)#exit
Console#show queue bandwidth                          4-185
Queue ID Weight
-----
0           16
1           64
2          128
3          240
Console#

```

Mapping Layer 3/4 Priorities to CoS Values

This switch supports several common methods of prioritizing layer 3/4 traffic to meet application requirements. Traffic priorities can be specified in the IP header of a frame, using the priority bits in the Type of Service (ToS) octet or the number of the TCP port. If priority bits are used, the ToS octet may contain three bits for IP Precedence or six bits for Differentiated Services Code Point (DSCP) service. When these services are enabled, the priorities are mapped to a Class of Service value by the switch, and the traffic then sent to the corresponding output queue.

Because different priority information may be contained in the traffic, this switch maps priority values to the output queues in the following manner:

- The precedence for priority mapping is IP Port Priority, IP Precedence or DSCP Priority, and then Default Port Priority.
- IP Precedence and DSCP Priority cannot both be enabled. Enabling one of these priority types will automatically disable the other.

Selecting IP Precedence/DSCP Priority

The switch allows you to choose between using IP Precedence or DSCP priority. Select one of the methods or disable this feature.

Command Attributes

- **Disabled** – Disables both priority services. (This is the default setting.)
- **IP Precedence** – Maps layer 3/4 priorities using IP Precedence.
- **IP DSCP** – Maps layer 3/4 priorities using Differentiated Services Code Point Mapping.

Web – Click Priority, IP Precedence/DSCP Priority Status. Select Disabled, IP Precedence or IP DSCP from the scroll-down menu.

IP Precedence/DSCP Priority Status

IP Precedence/DSCP Priority Status IP Precedence ▾

CLI – The following example enables IP Precedence service on the switch.

```
Console(config)#map ip precedence
Console(config)#
```

4-189

Mapping IP Precedence

The Type of Service (ToS) octet in the IPv4 header includes three precedence bits defining eight different priority levels ranging from highest priority for network control packets to lowest priority for routine traffic. The default IP Precedence values are mapped one-to-one to Class of Service values (i.e., Precedence value 0 maps to CoS value 0, and so forth). Bits 6 and 7 are used for network control, and the other bits for various application types. ToS bits are defined in the following table.

Priority Level	Traffic Type
7	Network Control
6	Internetwork Control
5	Critical
4	Flash Override
3	Flash
2	Immediate
1	Priority
0	Routine

Command Attributes

- **IP Precedence Priority Table** – Shows the IP Precedence to CoS map.
- **Class of Service Value** – Maps a CoS value to the selected IP Precedence value. Note that “0” represents low priority and “7” represent high priority.

Note: IP Precedence settings apply to all interfaces.

Web – Click Priority, IP Precedence Priority. Select a port or trunk from the Interface field. Select an entry from the IP Precedence Priority Table, enter a value in the Class of Service Value field, and then click Apply.

* Mapping specific values for IP Precedence is implemented as an interface configuration command, but any changes apply to the all interfaces on the switch.

CLI – The following example globally enables IP Precedence service on the switch, maps IP Precedence value 1 to CoS value 0 (on port 1), and then displays the IP Precedence settings.

```

Console(config)#map ip precedence                                4-189
Console(config)#interface ethernet 1/1                          4-119
Console(config-if)#map ip precedence 1 cos 0                    4-189
Console(config-if)#end
Console#show map ip precedence ethernet 1/5                     4-194
Precedence mapping status: disabled

  Port      Precedence COS
  -----
  Eth 1/ 1      0    0
  Eth 1/ 1      1    0
  Eth 1/ 1      2    2
  Eth 1/ 1      3    3
  Eth 1/ 1      4    4
  Eth 1/ 1      5    5
  Eth 1/ 1      6    6
  Eth 1/ 1      7    7
Console#
    
```

* Mapping specific values for IP Precedence is implemented as an interface configuration command, but any changes apply to the all interfaces on the switch.

Mapping DSCP Priority

The DSCP is six bits wide, allowing coding for up to 64 different forwarding behaviors. The DSCP replaces the ToS bits, but it retains backward compatibility with the three precedence bits so that non-DSCP compliant, ToS-enabled devices, will not conflict with the DSCP mapping. Based on network policies, different kinds of traffic can be marked for different kinds of forwarding. The DSCP default values are defined in the following table. Note that all the DSCP values that are not specified are mapped to CoS value 0.

IP DSCP Value	CoS Value
0	0
8	1
10, 12, 14, 16	2
18, 20, 22, 24	3
26, 28, 30, 32, 34, 36	4
38, 40, 42	5
48	6
46, 56	7

Command Attributes

- **DSCP Priority Table** – Shows the DSCP Priority to CoS map.
- **Class of Service Value** – Maps a CoS value to the selected DSCP Priority value. Note that “0” represents low priority and “7” represent high priority.

Note: IP DSCP settings apply to all interfaces.

Web – Click Priority, IP DSCP Priority. Select a port or trunk from the Interface field. Select an entry from the DSCP table, enter a value in the Class of Service Value field, then click Apply.

IP DSCP Priority

Interface

Port 1

Trunk

Select

DSCP Priority Table

DSCP 0 - CoS 0

DSCP 1 - CoS 0

DSCP 2 - CoS 0

DSCP 3 - CoS 0

DSCP 4 - CoS 0

DSCP 5 - CoS 0

DSCP 6 - CoS 0

Class of Service Value

1 (0-7)

Restore Default

* Mapping specific values for IP DSCP is implemented as an interface configuration command, but any changes will apply to the all interfaces on the switch.

CLI – The following example globally enables DSCP Priority service on the switch, maps DSCP value 0 to CoS value 1 (on port 1), and then displays the DSCP Priority settings.

Console(config)#map ip dscp4-191

Console(config)#interface ethernet 1/14-119

Console(config-if)#map ip dscp 1 cos 04-191

Console(config-if)#end

Console#show map ip dscp ethernet 1/54-195

DSCP mapping status: disabled

Port	DSCP	COS
Eth 1/ 1	0	0
Eth 1/ 1	1	0
Eth 1/ 1	2	0
Eth 1/ 1	3	0
:		
Eth 1/ 1	61	0
Eth 1/ 1	62	0
Eth 1/ 1	63	0

Console#

* Mapping specific values for IP DSCP is implemented as an interface configuration command, but any changes will apply to the all interfaces on the switch.

Mapping IP Port Priority

You can also map network applications to Class of Service values based on the IP port number (i.e., TCP/UDP port number) in the frame header. Some of the more common TCP service ports include: HTTP: 80, FTP: 21, Telnet: 23 and POP3: 110.

Command Attributes

- **IP Port Priority Status** – Enables or disables the IP port priority.
- **Interface** – Selects the port or trunk interface to which the settings apply.
- **IP Port Priority Table** – Shows the IP port to CoS map.
- **IP Port Number (TCP/UDP)** – Set a new IP port number.
- **Class of Service Value** – Sets a CoS value for a new IP port. Note that “0” represents low priority and “7” represent high priority.

Note: IP Port Priority settings apply to all interfaces.

Web – Click Priority, IP Port Status. Set IP Port Priority Status to Enabled.

IP Port Status

IP Port Priority Global Status Disabled

Click Priority, IP Port Priority. Select a port or trunk from the Interface field. Enter the port number for a network application in the IP Port Number box and the new CoS value in the Class of Service box, and then click Add IP Port.

- * Mapping specific values for IP Port Priority is implemented as an interface configuration command, but any changes will apply to the all interfaces on the switch.

CLI – The following example globally enables IP Port Priority service on the switch, maps HTTP traffic (on port 1) to CoS value 0, and then displays the IP Port Priority settings.

```

Console(config)#map ip port                                4-187
Console(config)#interface ethernet 1/1                    4-119
Console(config-if)#map ip port 80 cos 0                  4-188
Console(config-if)#end
Console#show map ip port ethernet 1/5                    4-193
TCP port mapping status: disabled

  Port          Port no. COS
  -----
  Eth 1/ 1      80    0
Console#
    
```

- * Mapping specific values for IP Port Priority is implemented as an interface configuration command, but any changes will apply to the all interfaces on the switch.

Copying IP Settings to Another Interface

You can copy IP Precedence, DSCP priority, or IP port priority settings from one interface (port or trunk) to other interfaces on the switch.

Command Attributes

- **Copy IP Precedence Priority Settings** – Selects IP Precedence priority settings to be copied to other interfaces.
- **Copy DSCP Priority Settings** – Selects DSCP priority settings to be copied to other interfaces.
- **Copy IP Port Priority Settings** – Selects IP port priority settings to be copied to other interfaces.
- **Source Interface** – Selects the port or trunk from which to copy priority settings.
- **Destination Interface** – Selects the port or trunk to which the priority settings will be copied. You can hold down the Ctrl key to select more than one port or trunk.

Web – Click Priority, Copy Settings. Mark the priority types to be copied, select the source and destination interface, then click Copy Settings.

Copy Settings

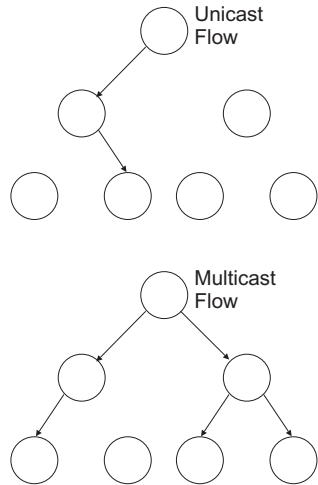
Copy IP Precedence Priority Settings	<input type="checkbox"/> Enabled	
Copy DSCP Priority Settings	<input type="checkbox"/> Enabled	
Copy IP Port Priority Settings	<input checked="" type="checkbox"/> Enabled	
Source Interface	<input checked="" type="radio"/> Port 1 <input type="radio"/> Trunk 	
Destination Interface	Port 1 2 3 4 5 6 7 8	Trunk

Copy Settings

CLI – Does not support this operation.

Multicast Filtering

Multicasting is used to support real-time applications such as videoconferencing or streaming audio. A multicast server does not have to establish a separate connection with each client. It merely broadcasts its service to the network, and any hosts that want to receive the multicast register with their local multicast switch/router. Although this approach reduces the network overhead required by a multicast server, the broadcast traffic must be carefully pruned at every multicast switch/router it passes through to ensure that traffic is only passed on the hosts which subscribed to this service.



This switch uses IGMP (Internet Group Management Protocol) to query for any attached hosts that want to receive a specific multicast service. It identifies the ports containing hosts requesting to join the service and sends data out to those ports only. It then propagates the service request up to any neighboring multicast switch/router to ensure that it will continue to receive the multicast service. This procedure is called multicast filtering.

The purpose of IP multicast filtering is to optimize a switched network's performance, so multicast packets will only be forwarded to those ports containing multicast group hosts or multicast routers/switches, instead of flooding traffic to all ports in the subnet (VLAN).

This switch not only supports IP multicast filtering by passively monitoring IGMP query and report messages and multicast routing probe messages to register end-stations as multicast group members, but also supports the DVMRP and PIM-DM multicast routing protocols required to forward multicast traffic to other subnets (page 3-222 and 3-231).

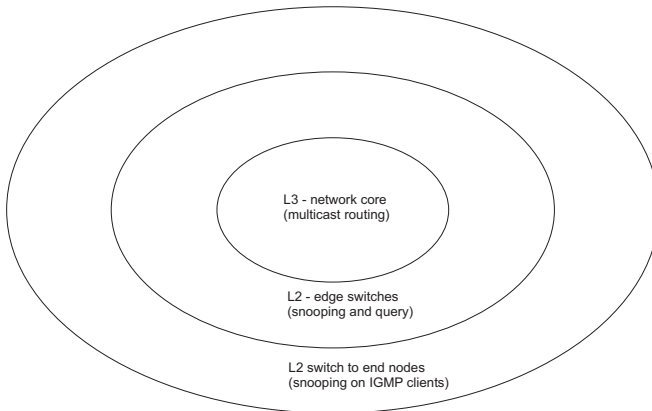
IGMP Protocol

The Internet Group Management Protocol (IGMP) runs between hosts and their immediately adjacent multicast router/switch. IGMP is a multicast host registration protocol that allows any host to inform its local router that it wants to receive transmissions addressed to a specific multicast group.

A router, or multicast-enabled switch, can periodically ask their hosts if they want to receive multicast traffic. If there is more than one router/switch on the LAN performing IP multicasting, one of these devices is elected “querier” and assumes the role of querying the LAN for group members. It then propagates the service requests on to any adjacent multicast switch/router to ensure that it will continue to receive the multicast service.

Based on the group membership information learned from IGMP, a router/switch can determine which (if any) multicast traffic needs to be forwarded to each of its ports. At Layer 3, multicast routers use this information, along with a multicast routing protocol such as DVMRP or PIM, to support IP multicasting across the Internet.

Note that IGMP neither alters nor routes IP multicast packets. A multicast routing protocol must be used to deliver IP multicast packets across different subnetworks. Therefore, when DVMRP or PIM routing is enabled for a subnet on this switch, you also need to enable IGMP.



Layer 2 IGMP (Snooping and Query)

IGMP Snooping and Query – If multicast routing is not supported on other switches in your network, you can use IGMP Snooping and IGMP Query (page 3-137) to monitor IGMP service requests passing between multicast clients and servers, and dynamically configure the switch ports which need to forward multicast traffic.

Static IGMP Router Interface – If IGMP snooping cannot locate the IGMP querier, you can manually designate a known IGMP querier (i.e., a multicast router/switch) connected over the network to an interface on your switch (page 3-140). This interface will then join all the current multicast groups supported by the attached router/switch to ensure that multicast traffic is passed to all appropriate interfaces within the switch.

Static IGMP Host Interface – For multicast applications that you need to control more carefully, you can manually assign a multicast service to specific interfaces on the switch (page 3-143).

IGMP Query (Layer 2 or 3) – IGMP Query can only be enabled globally at Layer 2, but can be enabled for individual VLAN interfaces at Layer 3 (page 3-144). However, note that Layer 2 query is disabled if Layer 3 query is enabled.

Configuring IGMP Snooping Parameters

You can configure the switch to forward multicast traffic intelligently. Based on the IGMP query and report messages, the switch forwards traffic only to the ports that request multicast traffic. This prevents the switch from broadcasting the traffic to all ports and possibly disrupting network performance.

Command Usage

- **IGMP Snooping** – This switch can passively snoop on IGMP Query and Report packets transferred between IP multicast routers/switches and IP multicast host groups to identify the IP multicast group members. It simply monitors the IGMP packets passing through it, picks out the group registration information, and configures the multicast filters accordingly.
- **IGMP Querier** – A router, or multicast-enabled switch, can periodically ask their hosts if they want to receive multicast traffic. If there is more than one router/switch on the LAN performing IP multicasting, one of these devices is elected “querier” and assumes the role of querying the LAN for group members. It then propagates the service requests on to any upstream multicast switch/router to ensure that it will continue to receive the multicast service.

Note: Multicast routers use this information, along with a multicast routing protocol such as DVMRP or PIM, to support IP multicasting across the Internet.

Command Attributes

- **IGMP Status** — When enabled, the switch will monitor network traffic to determine which hosts want to receive multicast traffic. This is also referred to as IGMP Snooping. (Default: Enabled)

- **Act as IGMP Querier** — When enabled, the switch can serve as the Querier, which is responsible for asking hosts if they want to receive multicast traffic. (Default: Disabled)
- **IGMP Query Count** — Sets the maximum number of queries issued for which there has been no response before the switch takes action to drop a client from the multicast group. (Range: 2-10, Default: 2)
- **IGMP Query Interval** — Sets the frequency at which the switch sends IGMP host-query messages. (Range: 60-125 seconds, Default: 125)
- **IGMP Report Delay** — Sets the time between receiving an IGMP Report for an IP multicast address on a port before the switch sends an IGMP Query out of that port and removes the entry from its list. (Range: 5-30 seconds, Default: 10)
- **Query Timeout** — The time the switch waits after the previous querier stops before it considers the router port (i.e., the interface which had been receiving query packets) to have expired. (Range: 300-500 seconds, Default: 300)
- **IGMP Version** — Sets the protocol version for compatibility with other devices on the network. (Default: 2, Range: 1 - 2)

Notes: 1. All systems on the subnet must support the same version.

2. Some attributes are only enabled for IGMPv2, including IGMP Report Delay and IGMP Query Timeout.

Web – Click IGMP Snooping, IGMP Configuration. Adjust the IGMP settings required, and click Apply. (The default settings are shown below.)

IGMP Configuration	
IGMP Status	<input checked="" type="checkbox"/> Enable
Act as IGMP Querier	<input type="checkbox"/> Enable
IGMP Query Count (2-10)	<input type="text" value="2"/>
IGMP Query Interval (60-125)	<input type="text" value="125"/> seconds
IGMP Report Delay (5-30)	<input type="text" value="10"/> seconds
IGMP Query Timeout (300-500)	<input type="text" value="300"/> seconds
IGMP Version	<input type="text" value="2"/>

CLI – This example modifies the settings for multicast filtering, and then displays the current status.

```

Console(config)#ip igmp snooping                                4-197
Console(config)#ip igmp snooping querier                        4-201
Console(config)#ip igmp snooping query-count 10                4-202
Console(config)#ip igmp snooping query-interval 100            4-203
Console(config)#ip igmp snooping query-max-response-time 20    4-203
Console(config)#ip igmp snooping query-time-out 300            4-204
Console(config)#ip igmp snooping version 2                     4-198
Console(config)#exit
Console#show ip igmp snooping                                   4-199
  Igmp Snooping Configuration
-----
Service status          : Enabled
Querier status          : Enabled
Query count             : 10
Query interval          : 100 sec
Query max response time : 20 sec
Query time-out          : 300 sec
IGMP snooping version   : Version 2
Console#

```

Displaying Interfaces Attached to a Multicast Router

Multicast routers that are attached to ports on the switch use information obtained from IGMP, along with a multicast routing protocol such as DVMRP or PIM, to support IP multicasting across the Internet. These routers may be dynamically discovered by the switch or statically assigned to an interface on the switch.

You can use the Multicast Router Port Information page to display the ports on this switch attached to a neighboring multicast router/switch for each VLAN ID.

Command Attributes

- **VLAN ID** – ID of configured VLAN (1-4094).
- **Multicast Router List** – Multicast routers dynamically discovered by this switch or those that are statically assigned to an interface on this switch.

Web – Click IGMP Snooping, Multicast Router Port Information. Select the required VLAN ID from the scroll-down list to display the associated multicast routers.

Multicast Router Port Information

VLAN ID: 1

Multicast Router List:

Unit1 Port11, Static

CLI – This example shows that Port 11 has been statically configured as a port attached to a multicast router.

```

Console#show ip igmp snooping mrouter vlan 1
VLAN M'cast Router Port Type
-----
1                Eth 1/11 Static
    
```

4-287

Specifying Static Interfaces for a Multicast Router

Depending on your network connections, IGMP snooping may not always be able to locate the IGMP querier. Therefore, if the IGMP querier is a known multicast router/ switch connected over the network to an interface (port or trunk) on your switch, you can manually configure the interface (and a specified VLAN) to join all the current multicast groups supported by the attached router. This can ensure that multicast traffic is passed to all the appropriate interfaces within the switch.

Command Attributes

- **Interface** – Activates the Port or Trunk scroll down list.
- **VLAN ID** – Selects the VLAN to propagate all multicast traffic coming from the attached multicast router.
- **Port or Trunk** – Specifies the interface attached to a multicast router.

Web – Click IGMP Snooping, Static Multicast Router Port Configuration. Specify the interfaces attached to a multicast router, indicate the VLAN which will forward all the corresponding multicast traffic, and then click Add. After you have finished adding interfaces to the list, click Apply.

Static Multicast Router Port Configuration

Current:

Vlan1, Unit1 Port11

New:

Interface	Port
VLAN ID	1
Port	1
Trunk	<input type="checkbox"/>

CLI – This example configures port 11 as a multicast router port within VLAN 1.

```

Console(config)#ip igmp snooping vlan 1 mrouter
ethernet 1/11
Console(config)#exit
Console#show ip igmp snooping mrouter vlan 1
VLAN M'cast Router Port Type
-----
1              Eth 1/11  Static
  
```

Displaying Port Members of Multicast Services

You can display the port members associated with a specified VLAN and multicast service.

Command Attribute

- **VLAN ID** – Selects the VLAN for which to display port members.
- **Multicast IP Address** – The IP address for a specific multicast service.
- **Multicast Group Port List** – Shows the interfaces that have already been assigned to the selected VLAN to propagate a specific multicast service.

Web – Click IGMP Snooping, IP Multicast Registration Table. Select a VLAN ID and the IP address for a multicast service from the scroll-down lists. The switch will display all the interfaces that are propagating this multicast service.

IP Multicast Registration Table

VLAN ID:

1

Multicast IP Address:

224.1.1.12

Multicast Group Port List:

Unit1 Port1, User

CLI – This example displays all the known multicast services supported on VLAN 1, along with the ports propagating the corresponding services. The Type field shows if this entry was learned dynamically or was statically configured.

Console#show bridge 1 multicast vlan 1

4-200

VLAN	M'cast IP addr.	Member ports	Type
1	224.1.1.12	Eth1/12	USER
1	224.1.1.2.3	Eth1/12	IGMP

Console#

Assigning Ports to Multicast Services

Multicast filtering can be dynamically configured using IGMP Snooping and IGMP Query messages as described in “Configuring IGMP Snooping Parameters” on page 3-137. For certain applications that require tighter control, you may need to statically configure a multicast service on the switch. First add all the ports attached to participating hosts to a common VLAN, and then assign the multicast service to that VLAN group.

Command Usage

- Static multicast addresses are never aged out.
- When a multicast address is assigned to an interface in a specific VLAN, the corresponding traffic can only be forwarded to ports within that VLAN.

Command Attribute

- **Interface** – Activates the Port or Trunk scroll down list.
- **VLAN ID** – Selects the VLAN to propagate all multicast traffic coming from the attached multicast router/switch.
- **Multicast IP** – The IP address for a specific multicast service
- **Port** or **Trunk** – Specifies the interface attached to a multicast router/switch.

Web – Click IGMP Snooping, IGMP Member Port Table. Specify the interface attached to a multicast service (via an IGMP-enabled switch or multicast router), indicate the VLAN that will propagate the multicast service, specify the multicast IP address, and click Add. After you have completed adding ports to the member list, click Apply.

IGMP Member Port Table											
<div> <div>IGMP Member Port List:</div> <div> <div>VLAN 1, 224.1.1.12, Unit 1, Port 1</div> <div> <div><<Add</div> <div>Remove</div> </div> </div> </div>											
<div> <div>New Static IGMP Member Port:</div> <table border="1"> <tr> <td>Interface</td> <td>Port ▾</td> </tr> <tr> <td>VLAN ID</td> <td>1 ▾</td> </tr> <tr> <td>Multicast IP</td> <td></td> </tr> <tr> <td>Port</td> <td>1 ▾</td> </tr> <tr> <td>Trunk</td> <td>▾</td> </tr> </table> </div>		Interface	Port ▾	VLAN ID	1 ▾	Multicast IP		Port	1 ▾	Trunk	▾
Interface	Port ▾										
VLAN ID	1 ▾										
Multicast IP											
Port	1 ▾										
Trunk	▾										

CLI – This example assigns a multicast address to VLAN 1, and then displays all the known multicast services supported on VLAN 1.

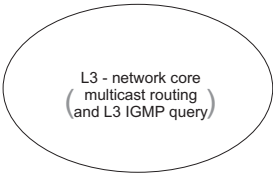
```
Console(config)#ip igmp snooping vlan 1 static 224.1.1.12      4-197
 ethernet 1/12
Console(config)#exit
Console#show mac-address-table multicast vlan 1                4-200
 VLAN M'cast IP addr. Member ports Type
-----
    1      224.1.1.12      Eth1/12      USER
    1      224.1.1.2.3     Eth1/12      IGMP
Console#
```

Layer 3 IGMP (Query used with Multicast Routing)

IGMP Snooping – IGMP Snooping is a Layer 2 function (page 3-137) that can be used to provide multicast filtering when no other switches in the network support multicast routing. (Note that IGMP Snooping can only be globally enabled.)

IGMP Query – Multicast query is used to poll each known multicast group for active members, and dynamically configure the switch ports which need to forward multicast traffic. Although the implementation differs slightly, IGMP Query is used in conjunction with both Layer 2 IGMP Snooping and multicast routing. Note that when using IGMP Snooping, multicast query is automatically enabled. (See “Configuring IGMP Snooping Parameters” on page 3-137.)

Layer 3 IGMP – This protocol includes a form of multicast query specifically designed to work with multicast routing. A router periodically asks its hosts if they want to receive multicast traffic. It then propagates service requests on to any upstream multicast router to ensure that it will continue to receive the multicast service. Layer 3 IGMP can be enabled for individual VLAN interfaces (page 3-144). (Note that Layer 2 snooping and query is disabled if Layer 3 IGMP is enabled.)



Configuring IGMP Interface Parameters

This switch uses IGMP (Internet Group Management Protocol) to query for any attached hosts that want to receive a specific multicast service. The hosts may respond with several types of IP multicast messages. Hosts respond to queries with report messages that indicate which groups they want to join or the groups to which they already belong. If a router does not receive a report message within a specified period of time, it will prune that interface from the multicast tree. A host can also submit a join message at any time without waiting for a query from the router. Host can also signal when they no longer want to receive traffic for a specific group by sending a leave-group message.

These IGMP messages are used by the router to identify ports containing multicast hosts and to restrict the downstream flow of multicast data to only these ports. If more than one router on the LAN is performing IP multicasting, one of these is elected as the “querier” and assumes the role of querying for group members. It then propagates the service request up to any neighboring multicast router to ensure that it will continue to receive the multicast service. The following parameters are used to control Layer 3 IGMP and query functions.

Command Attributes

- **VLAN** (Interface) – VLAN interface bound to a primary IP address.
(Range: 1-4094)
- **IGMP Protocol Status** (Admin Status) – Enables IGMP on a VLAN interface. (Default: Disabled)
- **Last Member Query Interval** – A multicast client sends an IGMP leave message when it leaves a group. The router then checks to see if this was the last host in the group by sending an IGMP query and starting a timer based on this command. If no reports are received before the timer expires, the group is deleted. (Range: 0-25 seconds; Default: 1 second)
 - This value may be tuned to modify the leave latency of the network. A reduced value results in reduced time to detect the loss of the last member of a group.

- **Max Query Response Time** – Configures the maximum response time advertised in IGMP queries. (Range: 0-25 seconds; Default: 10 seconds)
 - The switch must be using IGMPv2 for this command to take effect.
 - This command defines how long any responder (i.e., client or router) still in the group has to respond to a query message before the router deletes the group.
 - By varying the Maximum Query Response Time, you can tune the burstiness of IGMP messages passed on the subnet; where larger values make the traffic less bursty, as host responses are spread out over a larger interval.
 - The number of seconds represented by the maximum response interval must be less than the Query Interval.
- **Query Interval** – Configures the frequency at which host query messages are sent. (Range: 1-255; Default: 125 seconds)
 - Multicast routers send host query messages to determine the interfaces that are connected to downstream hosts requesting a specific multicast service. Only the designated multicast router for a subnet sends host query messages, which are addressed to the multicast address 224.0.0.1.
 - For IGMP Version 1, the designated router is elected according to the multicast routing protocol that runs on the LAN. But for IGMP Version 2, the designated querier is the lowest IP-addressed multicast router on the subnet.
- **Robustness Variable** – Specifies the robustness (i.e., expected packet loss) for this interface. The robustness value is used in calculating the appropriate range for other IGMP variables, such as the Group Membership Interval (**Last Member Query Interval**), as well as the Other Querier Present Interval, and the Startup Query Count (RFC 2236). (Range: 1-255; Default: 2)
- **Version** – Configures the IGMP version used on an interface. (Options: Version 1 or 2; Default: Version 2)
 - All routers on the subnet must support the same version. However, the multicast hosts on the subnet may support either IGMP version 1 or 2.
 - The switch must be set to version 2 to enable the **Max Query Response Time**.

- **Querier** – Device currently serving as the IGMP querier for this multicast service.

Web – Click IP, IGMP, Interface Settings. Specify each interface that will support IGMP (Layer 3), specify the IGMP parameters for each interface, then click Apply.

IGMP Interface Information								
Interface	Admin Status	Version	Robustness Variable	Query Interval	Max Query Response Time	Last Member Query Interval	Querier	Configure
VLAN2	Enabled	2	2	125	10	1	10.1.0.253	Configure
VLAN3	Enabled	2	2	125	10	1	10.1.5.253	Configure

Entry Count: 2

IGMP Interface Settings			
VLAN : <input type="text" value="2"/>			
IGMP Protocol Status	<input type="text" value="Enabled"/>	Query Interval (seconds)	<input type="text" value="125"/>
Last Member Query Interval (0 - 25 seconds)	<input type="text" value="1"/>	Robustness Variable (1 - 255)	<input type="text" value="2"/>
Max Query Response Time (0 - 25 seconds)	<input type="text" value="10"/>	Version	<input type="text" value="2"/>

CLI – This example configures the IGMP parameters for VLAN 1.

Console(config)#interface vlan 1	4-165
Console(config-if)#ip igmp	4-206
Console(config-if)#ip igmp last-memb-query-interval 10	4-209
Console(config-if)#ip igmp max-resp-interval 20	4-208
Console(config-if)#ip igmp query-interval 100	4-208
Console(config-if)#ip igmp robustval 3	4-207
Console(config-if)#ip igmp version 1	4-210
Console(config-if)#end	
Console#show ip igmp interface vlan 1	4-211
Vlan 1 is up	
IGMP is enable, version is 2	
Robustness variable is 2	
Query interval is 125 sec	
Query Max Response Time is 10 sec, Last Member Query Interval is 1 sec	
Querier is 10.1.0.253	
Console#	

Displaying Multicast Group Information

When IGMP (Layer 3) is enabled on this switch the current multicast groups learned via IGMP can be displayed in the IP/IGMP/Group Information page. When IGMP (Layer 3) is disabled and IGMP (Layer 2) is enabled, you can view the active multicast groups in the IGMP Snooping/IP Multicast Registration Table (see page 3-142).

Command Attributes

- **Group Address** – IP multicast group address with subscribers directly attached or downstream from this switch.
- **Interface** – The interface on this switch that has received traffic directed to the multicast group address.
- **Last Reporter** – The IP address of the source of the last membership report received for this multicast group address on this interface. If no membership report has been received, this object has the value 0.0.0.0.
- **Up time** – The time elapsed since this entry was created.
- **Expire** – The time remaining before this entry will be aged out. (Default: 260 seconds)

- **V1 Timer** – The time remaining until the switch assumes that there are no longer any IGMP Version 1 members on the IP subnet attached to this interface. (Default: 400 seconds)
 - If the switch receives an IGMP Version 1 Membership Report, it sets a timer to note that there are Version 1 hosts present which are members of the group for which it heard the report.
 - If there are Version 1 hosts present for a particular group, the switch will ignore any Leave Group messages that it receives for that group.

Web – Click IP, IGMP, IGMP Group Information.

IGMP Group Membership					
Group Address	Interface	Last Reporter	Up time	Expire	V1 Timer
234.5.6.7	VLAN2	10.1.0.19	6077	209	0
234.5.6.8	VLAN3	10.1.5.19	6067	226	0

Entry Count: 2

CLI – The following shows the IGMP groups currently active on VLAN 1.

Console#show ip igmp groups vlan 1						4-213
GroupAddress	InterfaceVlan	Lastreporter	Uptime	Expire	VlTimer	
234.5.6.8	1	10.1.5.19	7068	220	0	
Console#						

IP Routing

Overview

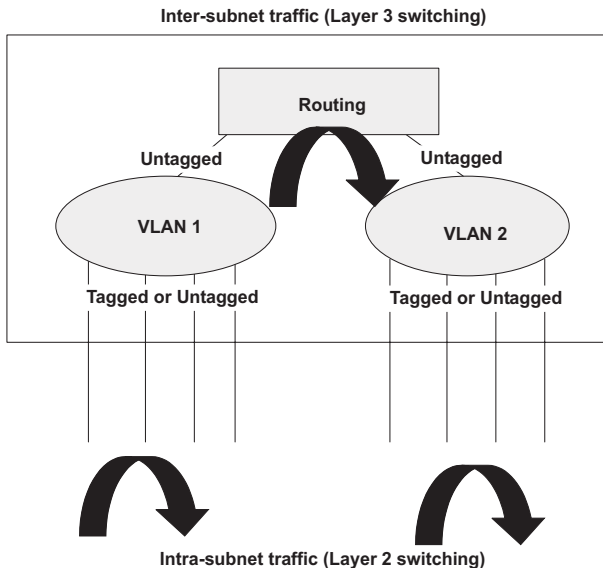
This switch supports IP routing and routing path management via static routing definitions (page 3-172) and dynamic routing such as RIP (page 3-175) or OSPF (page 3-186). When IP routing is enabled (page 3-176), this switch acts as a wire-speed router, passing traffic between VLANs using different IP interfaces, and routing traffic to external IP

networks. However, when the switch is first booted, no default routing is defined. As with all traditional routers, the routing functions must first be configured to work.

Initial Configuration

In the default configuration, all ports belong to the same VLAN and the switch provides only Layer 2 functionality. Therefore, first create VLANs for each unique user group or application traffic (page 3-110), assign all ports that belong to the same group to these VLANs (page 3-111), and then assign an IP interface to each VLAN (page 3-155). By separating the network into different VLANs, it can be partitioned into subnetworks that are disconnected at Layer 2. Network traffic within the same subnet is still switched using Layer 2 switching. And the VLANs can now be interconnected (only as required) with Layer 3 switching.

Each VLAN represents a virtual interface to Layer 3. You just need to provide the network address for each virtual interface, and the traffic between different subnetworks will be routed by Layer 3 switching.



IP Switching

IP Switching (or packet forwarding) encompasses tasks required to forward packets for both Layer 2 and Layer 3, as well as traditional routing. These functions include:

- Layer 2 forwarding (switching) based on the Layer 2 destination MAC address
- Layer 3 forwarding (routing):
 - Based on the Layer 3 destination address
 - Replacing destination/source MAC addresses for each hop
 - Incrementing the hop count
 - Decrementing the time-to-live
 - Verifying and recalculating the Layer 3 checksum

If the destination node is on the same subnetwork as the source network, then the packet can be transmitted directly without the help of a router. However, if the MAC address is not yet known to the switch, an Address Resolution Protocol (ARP) packet with the destination IP address is broadcast to get the destination MAC address from the destination node. The IP packet can then be sent directly with the destination MAC address.

If the destination belongs to a different subnet on this switch, the packet can be routed directly to the destination node. However, if the packet belongs to a subnet not included on this switch, then the packet should be sent to a router (with the MAC address of the router itself used as the destination MAC address, and the destination IP address of the destination node). The router will then forward the packet to the destination node via the correct path. The router can also use the ARP protocol to find out the MAC address of the destination node of the next router as necessary.

Note: In order to perform IP switching, the switch should be recognized by other network nodes as an IP router, either by setting it as the default gateway or by redirection from another router via the ICMP process.

When the switch receives an IP packet addressed to its own MAC address, the packet follows the Layer 3 routing process. The destination IP address is checked against the Layer 3 address table. If the address is not already

there, the switch broadcasts an ARP packet to all the ports on the destination VLAN to find out the destination MAC address. After the MAC address is discovered, the packet is reformatted and sent out to the destination. The reformat process includes decreasing the Time-To-Live (TTL) field of the IP header, recalculating the IP header checksum, and replacing the destination MAC address with either the MAC address of the destination node or that of the next hop router.

When another packet destined to the same node arrives, the destination MAC can be retrieved directly from the Layer 3 address table; the packet is then reformatted and sent out the destination port. IP switching can be done at wire-speed when the destination address entry is already in the Layer 3 address table.

If the switch determines that a frame must be routed, the route is calculated only during setup. Once the route has been determined, all packets in the current flow are simply switched or forwarded across the chosen path. This takes advantage of the high throughput and low latency of switching by enabling the traffic to bypass the routing engine once the path calculation has been performed.

Routing Path Management

Routing Path Management involves the determination and updating of all the routing information required for packet forwarding, including:

- Handling routing protocols
- Updating the routing table
- Updating the Layer 3 switching database

Routing Protocols

The switch supports both static and dynamic routing.

- Static routing requires routing information to be stored in the switch either manually or when a connection is set up by an application outside the switch.

- Dynamic routing uses a routing protocol to exchange routing information, calculate routing tables, and respond to changes in the status or loading of the network.

The switch supports RIP, RIP-2 and OSPFv2 dynamic routing protocols.

RIP and RIP-2 Dynamic Routing Protocols

The RIP protocol is the most widely used routing protocol. RIP uses a distance-vector-based approach to routing. Routes are determined on the basis of minimizing the distance vector, or hop count, which serves as a rough estimate of transmission cost. Each router broadcasts its advertisement every 30 seconds, together with any updates to its routing table. This allows all routers on the network to learn consistent tables of next hop links which lead to relevant subnets.

OSPFv2 Dynamic Routing Protocol

OSPF overcomes all the problems of RIP. It uses a link state routing protocol to generate a shortest-path tree, then builds up its routing table based on this tree. OSPF produces a more stable network because the participating routers act on network changes predictably and simultaneously, converging on the best route more quickly than RIP. Moreover, when several equal-cost routes to a destination exist, traffic can be distributed equally among them.

Non-IP Protocol Routing

The switch supports IP routing only. Non-IP protocols such as IPX and Appletalk cannot be routed by this switch, and will be confined within their local VLAN group unless bridged by an external router.

To coexist with a network built on multilayer switches, the subnetworks for non-IP protocols must follow the same logical boundary as that of the IP subnetworks. A separate multi-protocol router can then be used to link the subnetworks by connecting to one port from each available VLAN on the network.

Basic IP Interface Configuration

To allow routing between different IP subnets, you must enable IP Routing as described in this section. You also need to define a VLAN for each IP subnet that will be connected directly to this switch. Note that you must first create a VLAN as described under “Creating VLANs” on page 3-110 before configuring the corresponding subnet. Remember that if you need to manage the switch in-band then you must define the IP subnet address for at least one VLAN.

Command Attributes

- **IP Routing Status** – Configures the switch to operate as a Layer 2 switch or as a multilayer routing switch. (Options: Disable this field to restrict operation to Layer 2 switching; enable it to allow multilayer operation at either Layer 2 or 3 as required.)
 - This command affects both static and dynamic unicast routing.
 - If IP routing is enabled, all IP packets are routed using either static routing or dynamic routing via RIP or OSPF, and other packets for all non-IP protocols (e.g., NetBuei, NetWare or AppleTalk) are switched based on MAC addresses. If IP routing is disabled, all packets are switched, with filtering and forwarding decisions based strictly on MAC addresses.
- **Default Gateway** – The routing device to which the switch will pass packets for all unknown subnets; i.e., packets that do not match any routing table entry. (Valid IP addresses consist of four numbers, 0 to 255, separated by periods.)

Web - Click IP, General, Global Settings. Set IP Routing Status to Disabled to restrict operation to Layer 2, or Enabled to allow multilayer switching, specify the default gateway which will be forwarded packets for all unknown subnets, and click Apply.

Global Settings

IP Routing Status	Enabled ▾
Default Gateway	10.1.0.254

Clear default gateway

CLI - This example enables IP routing, and sets the default gateway.

Console(config)#ip routing	4-226
Console(config)#ip route default 10.1.0.254	4-227

Configuring IP Routing Interfaces

You can specify the IP subnets connected to this router by manually assigning an IP address to each VLAN, or by using the RIP or OSPF dynamic routing protocol to identify routes that lead to other interfaces by exchanging protocol messages with other routers on the network.

Command Usage

- If this router is directly connected to end node devices (or connected to end nodes via shared media) that will be assigned to a specific subnet, then you must create a router interface for each VLAN that will support routing. The router interface consists of an IP address and subnet mask. This interface address defines both the network number to which the router interface is attached and the router's host number on that network. In other words, a router interface address defines the network and subnetwork numbers of the segment that is connected to that interface, and allows you to send IP packets to or from the router.

- Before you configure any network interfaces on this router, you should first create a VLAN for each unique user group, or for each network application and its associated users. Then assign the ports associated with each of these VLANs.

Command Attributes

- **VLAN ID** – ID of configured VLAN (1-4094, no leading zeroes).
- **IP Address Mode** – Specifies whether the IP address for this interface is statically assigned, or obtained from a network address server. (Options: Static, DHCP - Dynamic Host Configuration Protocol, BOOTP - Boot Protocol; Default: Static)
 - If Static address type is selected, then you must also specify whether the IP address is the primary IP address on the VLAN or a secondary IP address. An interface can have only one primary IP address, but can have multiple secondary IP addresses. In other words, you will need to specify secondary addresses if more than one IP subnet can accessed via this interface.
 - If DHCP/BOOTP is enabled, IP will not function until a reply has been received from the address server. Requests will be broadcast periodically by the router for an IP address. (DHCP/BOOTP values include the IP address and subnet mask.)
- **IP Address** – Address of the VLAN interface. Valid IP addresses consist of four numbers, 0 to 255, separated by periods.
- **Subnet Mask** – This mask identifies the host address bits used for routing to specific subnets.

Web - Click IP, General, Routing Interface. Specify an IP interface for each VLAN that will support routing to other subnets. First specify a primary address, and click Set IP Configuration. If you need to assign secondary addresses, enter these addresses one at a time, and click Set IP Configuration after entering each address.

Routing Interface

VLAN	1
IP Address Mode	Static Primary
IP Address	10.1.0.253
Subnet Mask	255.255.255.0

CLI - This example sets a primary IP address for VLAN 1, and then adds a secondary IP address for a different subnet also attached to this router interface.

```

Console(config)#interface vlan 1
Console(config-if)#ip address 10.1.0.253 255.255.255.0      4-216
Console(config-if)#ip address 10.1.9.253 255.255.255.0 secondary
Console(config-if)#

```

Address Resolution Protocol

If IP routing is enabled (page 3-154), the router uses its routing tables to make routing decisions, and uses Address Resolution Protocol (ARP) to forward traffic from one hop to the next. ARP is used to map an IP address to a physical layer (i.e., MAC) address. When an IP frame is received by this router (or any standards-based router), it first looks up the MAC address corresponding to the destination IP address in the ARP cache. If the address is found, the router writes the MAC address into the

appropriate field in the frame header, and forwards the frame on to the next hop. IP traffic passes along the path to its final destination in this way, with each routing device mapping the destination IP address to the MAC address of the next hop toward the recipient, until the packet is delivered to the final destination.

If there is no entry for an IP address in the ARP cache, the router will broadcast an ARP request packet to all devices on the network. The ARP request contains the following fields similar to that shown in this example:

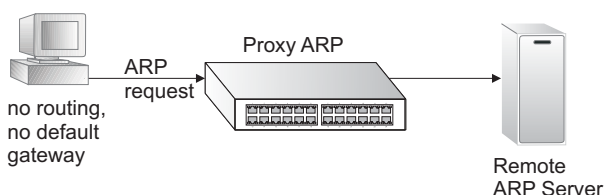
destination IP address	10.1.0.19
destination MAC address	?
source IP address	10.1.0.253
source MAC address	00-00-ab-cd-00-00

When devices receive this request, they discard it if their address does not match the destination IP address in the message. However, if it does match, they write their own hardware address into the destination MAC address field and send the message back to the source hardware address. When the source device receives a reply, it writes the destination IP address and corresponding MAC address into its cache, and forwards the IP traffic on to the next hop. As long as this entry has not timed out, the router will be able forward traffic directly to the next hop for this destination without having to broadcast another ARP request.

Proxy ARP

When a node in the attached subnetwork does not have routing or a default gateway configured, Proxy ARP can be used to forward ARP requests to a remote subnetwork. When the router receives an ARP request for a remote network and Proxy ARP is enabled, it determines if it has the best route to the remote network, and then answers the ARP

request by sending its own MAC address to the requesting node. That node then sends traffic to the router, which in turn uses its own routing table to forward the traffic to the remote destination.



Basic ARP Configuration

You can use the ARP General configuration menu to specify the timeout for ARP cache entries, or to enable Proxy ARP for specific VLAN interfaces.

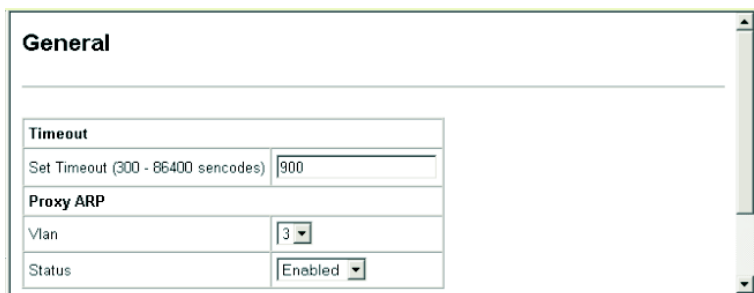
Command Usage

- The aging time determines how long dynamic entries remain the cache. If the timeout is too short, the router may tie up resources by repeating ARP requests for addresses recently flushed from the table.
- End stations that require Proxy ARP must view the entire network as a single network. These nodes must therefore use a smaller subnet mask than that used by the router or other relevant network devices.
- Extensive use of Proxy ARP can degrade router performance because it may lead to increased ARP traffic and increased search time for larger ARP address tables.

Command Attributes

- **Timeout** – Sets the aging time for dynamic entries in the ARP cache. (Range: 300 - 86400 seconds; Default: 1200 seconds or 20 minutes)
- **Proxy ARP** – Enables or disables Proxy ARP for specified VLAN interfaces.

Web - Click IP, ARP, General. Set the timeout to a suitable value for the ARP cache, enable Proxy ARP for subnetworks that do not have routing or a default gateway, and click Apply.



The screenshot shows a web interface for configuring the switch's ARP settings. The 'General' tab is selected. Under the 'Timeout' section, 'Set Timeout (300 - 86400 seconds)' is set to 900. Under the 'Proxy ARP' section, 'Vlan' is set to 3 and 'Status' is set to 'Enabled'.

CLI - This example sets the ARP cache timeout for 15 minutes (i.e., 900 seconds), and enables Proxy ARP for VLAN 3.

```
Console(config)#arp-timeout 900                                4-223
Console(config)#interface vlan 3                               4-119
Console(config-if)#ip proxy-arp                                4-224
Console(config-if)#
```

Configuring Static ARP Addresses

For devices that do not respond to ARP requests, traffic will be dropped because the IP address cannot be mapped to a physical address. If this occurs, you can manually map an IP address to the corresponding physical address in the ARP.

Command Usage

- You can define up to 128 static entries in the ARP cache.
- Static entries will not be aged out or deleted when power is reset. You can only remove a static entry via the configuration interface.

Command Attributes

- **IP Address** – IP address statically mapped to a physical MAC address. (Valid IP addresses consist of four numbers, 0 to 255, separated by periods.)

- **MAC Address** – MAC address statically mapped to the corresponding IP address. (Valid MAC addresses are hexadecimal numbers in the format: xx-xx-xx-xx-xx-xx.)
- **Entry Count** – The number of static entries in the ARP cache.

Web - Click IP, ARP, Static Addresses. Enter the IP address, the corresponding MAC address, and click Apply.

CLI - This example sets a static entry for the ARP cache.

```
Console(config)#arp 10.1.0.11 00-11-22-33-44-55
Console(config)#
```

4-222

Displaying Dynamically Learned ARP Entries

The ARP cache contains entries that map IP addresses to the corresponding physical address. Most of these entries will be dynamically learned through replies to broadcast messages. You can display all of the dynamic entries in the ARP cache, change specific dynamic entries into static entries, or clear all dynamic entries from the cache.

Command Attributes

- **IP Address** – IP address of a dynamic entry in the cache.
- **MAC Address** – MAC address mapped to the corresponding IP address.
- **Interface** – VLAN interface associated with the address entry.

- **Dynamic to Static*** – Changes a selected dynamic entry to a static entry.
- **Clear All*** – Deletes all dynamic entries from the ARP cache.
- **Entry Count** – The number of dynamic entries in the ARP cache.

* These buttons take effect immediately. You are not prompted to confirm the action.

Web - Click IP, ARP, Dynamic Addresses. You can use the buttons provided to change a dynamic entry to a static entry, or to clear all dynamic entries in the cache.

Dynamic Addresses

Current:		
IP address, MAC address, Interface		
10.1.0.19, 00-10-B5-62-03-74, 1		

Dynamic to Static

Clear All

Entry Count: 1

CLI - This example shows all entries in the ARP cache.

```

Console#show arp
Arp cache timeout: 1200 (seconds)
4-224

  IP Address      MAC Address      Type      Interface
  -----
    10.1.0.0     ff-ff-ff-ff-ff-ff  other          1
    10.1.0.11    00-11-22-33-44-55  static         1
    10.1.0.12    01-02-03-04-05-06  static         1
    10.1.0.19    00-10-b5-62-03-74  dynamic        1
    10.1.0.253   00-00-ab-cd-00-00  other          1
    10.1.0.255   ff-ff-ff-ff-ff-ff  other          1

Total entry : 6
Console#clear arp-cache
This operation will delete all the dynamic entries in ARP Cache.
Are you sure to continue this operation (y/n)?y
Console#
4-223
    
```

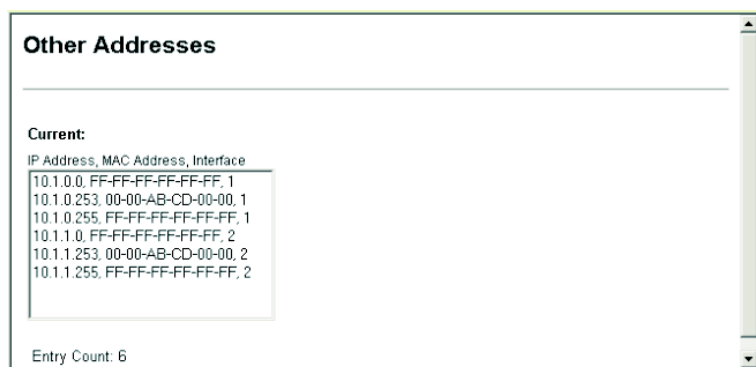
Displaying Local ARP Entries

The ARP cache also contains entries for local interfaces, including subnet, host, and broadcast addresses.

Command Attributes

- **IP Address** – IP address of a local entry in the cache.
- **MAC Address** – MAC address mapped to the corresponding IP address.
- **Interface** – VLAN interface associated with the address entry.
- **Entry Count** – The number of local entries in the ARP cache.

Web - Click IP, ARP, Other Addresses.



CLI - This router uses the Type specification “other” to indicate local cache entries in the ARP cache.

Console#show arp				4-224
Arp cache timeout: 1200 (seconds)				
IP Address	MAC Address	Type	Interface	
10.1.0.0	ff-fF-fF-fF-fF-fF	other	1	
10.1.0.11	00-11-22-33-44-55	static	1	
10.1.0.12	01-02-03-04-05-06	static	1	
10.1.0.19	00-10-b5-62-03-74	dynamic	1	
10.1.0.253	00-00-ab-cd-00-00	other	1	
10.1.0.255	ff-fF-fF-fF-fF-fF	other	1	
Total entry : 6				
Console#				

Displaying ARP Statistics

You can display statistics for ARP messages crossing all interfaces on this router.

Statistical Values

Parameter	Description
Received Request	Number of ARP Request packets received by the router.
Received Reply	Number of ARP Reply packets received by the router.
Sent Request	Number of ARP Request packets sent by the router.
Sent Reply	Number of ARP Reply packets sent by the router.

Web - Click IP, ARP, Statistics.



The screenshot shows a web interface titled "ARP Statistics". It contains a table with two main sections: "Received" and "Sent". Each section has two rows: "Request" and "Reply". The values for "Received" are 31 for Request and 4 for Reply. The values for "Sent" are 53 for Request and 31 for Reply.

ARP Statistics	
<hr/>	
Received	
Request	31
Reply	4
Sent	
Request	53
Reply	31

CLI - This example provides detailed statistics on common IP-related protocols.

```

Console#show ip traffic
IP statistics:
  Rcvd: 5 total, 5 local destination
        0 checksum errors
        0 unknown protocol, 0 not a gateway
  Frags: 0 reassembled, 0 timeouts
        0 fragmented, 0 couldn't fragment
  Sent: 9 generated
        0 no route
ICMP statistics:
  Rcvd: 0 checksum errors, 0 redirects, 0 unreachable, 0 echo
        5 echo reply, 0 mask requests, 0 mask replies, 0 quench
        0 parameter, 0 timestamp
  Sent: 0 redirects, 0 unreachable, 0 echo, 0 echo reply
        0 mask requests, 0 mask replies, 0 quench, 0 timestamp
        0 time exceeded, 0 parameter problem
UDP statistics:
  Rcvd: 0 total, 0 checksum errors, 0 no port
  Sent: 0 total
TCP statistics:
  Rcvd: 0 total, 0 checksum errors
  Sent: 0 total
ARP statistics:
  Rcvd: 0 requests, 1 replies
  Sent: 1 requests, 0 replies
  
```

Displaying Statistics for IP Protocols

IP Statistics

The Internet Protocol (IP) provides a mechanism for transmitting blocks of data (often called packets or frames) from a source to a destination, where these network devices (i.e., hosts) are identified by fixed length addresses. The Internet Protocol also provides for fragmentation and reassembly of long packets, if necessary, for transmission through “small packet” networks.

Statistical Values

Parameter	Description
Packets Received	The total number of input datagrams received from interfaces, including those received in error.
Received Address Errors	The number of input datagrams discarded because the IP address in the header's destination field was not a valid address for this entity.
Received Packets Discarded	The number of input datagrams for which no problems were encountered to prevent their continued processing, but which were discarded (e.g., for lack of buffer space).
Output Requests	The total number of datagrams which local IP user-protocols (including ICMP) supplied to IP in requests for transmission.
Output Packet No Route	The number of datagrams discarded because no route could be found to transmit them to their destination. Note that this includes any datagrams which a host cannot route because all of its default gateways are down.
Datagrams Forwarded	The number of input datagrams for which this entity was not their final IP destination, as a result of which an attempt was made to find a route to forward them to that final destination.
Reassembly Required	The number of IP fragments received which needed to be reassembled at this entity.
Reassembly Failures	The number of failures detected by the IP re-assembly algorithm (for whatever reason: timed out, errors, etc.).
Datagrams Failing Fragmentation	The number of datagrams that have been discarded because they needed to be fragmented at this entity but could not be, e.g., because their "Don't Fragment" flag was set.
Received Header Errors	The number of input datagrams discarded due to errors in their IP headers, including bad checksums, version number mismatch, other format errors, time-to-live exceeded, errors discovered in processing their IP options, etc.

Parameter	Description
Unknown Protocols Received	The number of locally-addressed datagrams received successfully but discarded because of an unknown or unsupported protocol.
Received Packets Delivered	The total number of input datagrams successfully delivered to IP user-protocols (including ICMP).
Discarded Output Packets	The number of output IP datagrams for which no problem was encountered to prevent their transmission to their destination, but which were discarded (e.g., for lack of buffer space).
Fragments Created	The number of datagram fragments that have been generated as a result of fragmentation at this entity.
Routing Discards	The number of routing entries which were chosen to be discarded even though they are valid. One possible reason for discarding such an entry could be to free-up buffer space for other routing entries.
Reassembly Successful	The number of datagrams successfully re-assembled.
Datagrams Successfully Fragmented	The number of IP datagrams that have been successfully fragmented at this entity.

Web - Click IP, Statistics, IP.

IP Statistics			
Packets Received	2367	Received Header Errors	0
Received Address Errors	0	Unknown Protocols Received	0
Received Packets Discarded	0	Received Packets Delivered	2364
Output Requests	2670	Discarded Output Packets	0
Output Packet No Route	2	Fragments Created	0
Datagrams Forwarded	3	Routing Discards	0
Reassembly Required	0	Reassembly Successful	0
Reassembly Failures	0	Datagrams Successfully Fragmented	0
Datagrams Failing Fragmentation	0		

CLI - See the example on page 3-164.

ICMP Statistics

Internet Control Message Protocol (ICMP) is a network layer protocol that transmits message packets to report errors in processing IP packets. ICMP is therefore an integral part of the Internet Protocol. ICMP messages may be used to report various situations, such as when a datagram cannot reach its destination, when the gateway does not have the buffering capacity to forward a datagram, and when the gateway can direct the host to send traffic on a shorter route. ICMP is also used by routers to feed back information about more suitable routes (i.e., the next hop router) to use for a specific destination.

Statistical Values

Parameter	Description
Messages	The total number of ICMP messages which the entity received/sent.
Errors	The number of ICMP messages which the entity received/sent but determined as having ICMP-specific errors (bad ICMP checksums, bad length, etc.).
Destination Unreachable	The number of ICMP Destination Unreachable messages received/sent.
Time Exceeded	The number of ICMP Time Exceeded messages received/sent.
Parameter Problems	The number of ICMP Parameter Problem messages received/sent.
Source Quenches	The number of ICMP Source Quench messages received/sent.
Redirects	The number of ICMP Redirect messages received/sent.
Echos	The number of ICMP Echo (request) messages received/sent.
Echo Replies	The number of ICMP Echo Reply messages received/sent.
Timestamps	The number of ICMP Timestamp (request) messages received/sent.

Parameter	Description
Timestamp Replies	The number of ICMP Timestamp Reply messages received/sent.
Address Masks	The number of ICMP Address Mask Request messages received/sent.
Address Mask Replies	The number of ICMP Address Mask Reply messages received/sent.

Web - Click IP, Statistics, ICMP.

ICMP Statistics		
	Received	Sent
Messages	0	4
Errors	0	0
Destination Unreachable	0	4
Time Exceeded	0	0
Parameter Problems	0	0
Source Quenchs	0	0
Redirects	0	0
Echos	0	0
Echo Replies	0	0
Timestamps	0	0
Timestamp Replies	0	0
Address Masks	0	0
Address Mask Replies	0	0

CLI - See the example on page 3-164.

UDP Statistics

User Datagram Protocol (UDP) provides a datagram mode of packet-switched communications. It uses IP as the underlying transport mechanism, providing access to IP-like services. UDP packets are delivered just like IP packets – connection-less datagrams that may be discarded before reaching their targets. UDP is useful when TCP would be too complex, too slow, or just unnecessary.

Statistical Values

Parameter	Description
Datagrams Received	The total number of UDP datagrams delivered to UDP users.
Datagrams Sent	The total number of UDP datagrams sent from this entity.
Receive Errors	The number of received UDP datagrams that could not be delivered for reasons other than the lack of an application at the destination port.
No Ports	The total number of received UDP datagrams for which there was no application at the destination port.

Web - Click IP, Statistics, UDP.

UDP Statistics			
Datagrams Received	174	Receive Errors	0
Datagrams Sent	0	No Ports	174

CLI - See the example on page 3-164.

TCP Statistics

The Transmission Control Protocol (TCP) provides highly reliable host-to-host connections in packet-switched networks, and is used in conjunction with IP to support a wide variety of Internet protocols.

Statistical Values

Parameter	Description
Segments Received	The total number of segments received, including those received in error. This count includes segments received on currently established connections.
Segments Sent	The total number of segments sent, including those on current connections but excluding those containing only retransmitted octets.
Active Opens	The number of times TCP connections have made a direct transition to the SYN-SENT state from the CLOSED state.
Failed Connection Attempts	The number of times TCP connections have made a direct transition to the CLOSED state from either the SYN-SENT state or the SYN-RCVD state, plus the number of times TCP connections have made a direct transition to the LISTEN state from the SYN-RCVD state.
Current Connections	The number of TCP connections for which the current state is either ESTABLISHED or CLOSE- WAIT.
Receive Errors	The total number of segments received in error (e.g., bad TCP checksums).
Segments Retransmitted	The total number of segments retransmitted - that is, the number of TCP segments transmitted containing one or more previously transmitted octets.
Passive Opens	The number of times TCP connections have made a direct transition to the SYN-RCVD state from the LISTEN state.
Reset Connections	The number of times TCP connections have made a direct transition to the CLOSED state from either the ESTABLISHED state or the CLOSE-WAIT state.

Web - Click IP, Statistics, TCP.

TCP Statistics			
Segments Received	3406	Receive Errors	0
Segments Sent	4162	Segments Retransmitted	0
Active Opens	0	Passive Opens	418
Failed Connection Attempts	0	Reset Connections	2
Current Connections	1		

CLI - See the example on page 3-164.

Configuring Static Routes

This router can dynamically configure routes to other network segments using dynamic routing protocols (i.e., RIP or OSPF). However, you can also manually enter static routes in the routing table. Static routes may be required to access network segments where dynamic routing is not supported, or can be set to force the use of a specific route to a subnet, rather than using dynamic routing. Static routes do not automatically change in response to changes in network topology, so you should only configure a small number of stable routes to ensure network accessibility.

Command Attributes

- **Interface** – Index number of the IP interface.
- **IP Address** – IP address of the destination network, subnetwork, or host.
- **Netmask** – Network mask for the associated IP subnet. This mask identifies the host address bits used for routing to specific subnets.
- **Gateway** – IP address of the gateway used for this route.
- **Metric** – Cost for this interface. This cost is only used if a route is imported by a dynamic routing protocol such as OSPF. (Range: 1-5, default: 1)
- **Entry Count** – The number of table entries.

Web - Click IP, Routing, Static Routes.

Static Routes

Current:

Interface, IP Address, Netmask, Nexthop, Metric

1	0.0.0.0	0.0.0.0	10.1.0.254	1
---	---------	---------	------------	---

<< Add
Remove

Clear all static routes

Entry Count: 1

New:

IP Address	<input style="width: 90%;" type="text"/>
Netmask	<input style="width: 90%;" type="text"/>
Nexthop	<input style="width: 90%;" type="text"/>
Metric	<input style="width: 80%;" type="text" value="1"/>

CLI - This example forwards all traffic for subnet 192.168.1.0 to the router 192.168.5.254, using the default metric of 1.

```

Console(config)#ip route 192.168.1.0 255.255.255.0
192.168.5.254
Console(config)#
  
```

4-227

Displaying the Routing Table

You can display all the routes that can be accessed via the local network interfaces, via static routes, or via a dynamically learned route. If route information is available through more than one of these methods, the priority for route selection is local, static, and then dynamic. Also note that the route for a local interface is not enabled (i.e., listed in the routing table) unless there is at least one active link connected to that interface.

Command Attributes

- **Interface** – Index number of the IP interface.
- **IP Address** – IP address of the destination network, subnetwork, or host. Note that the address 0.0.0.0 indicates the default gateway for this router.

- **Netmask** – Network mask for the associated IP subnet. This mask identifies the host address bits used for routing to specific subnets.
- **Next Hop** – The IP address of the next hop (or gateway) in this route.
- **Protocol** – The protocol which generated this route information. (Options: local, static, RIP, OSPF)
- **Metric** – Cost for this interface.
- **Entry Count** – The number of table entries.

Web - Click IP, Routing, Routing Table.

Routing Table

Current:

Interface	IP Address	Netmask	Next Hop	Protocol	Metric
1	0.0.0.0	0.0.0.0	10.1.0.254	static	1
1	10.1.0.0	255.255.255.0	10.1.0.253	local	1
1	10.1.1.0	255.255.255.0	10.1.0.254	RIP	2

[Clear all dynamic routes](#)

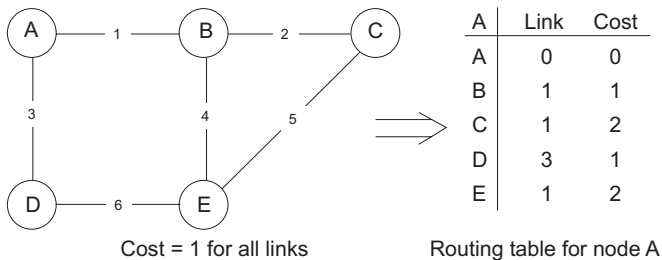
Entry Count: 3

CLI - This example shows routes obtained from various methods.

Console#show ip route						4-228
Ip Address	Netmask	Next Hop	Protocol	Metric	Interface	
0.0.0.0	0.0.0.0	10.1.0.254	static	1	1	
10.1.0.0	255.255.255.0	10.1.0.253	local	1	1	
10.1.1.0	255.255.255.0	10.1.0.254	RIP	2	1	
Total entries: 3						
Console#						

Configuring the Routing Information Protocol

The RIP protocol is the most widely used routing protocol. The RIP protocol uses a distance-vector-based approach to routing. Routes are determined on the basis of minimizing the distance vector, or hop count, which serves as a rough estimate of transmission cost. Each router broadcasts its advertisement every 30 seconds, together with any updates to its routing table. This allows all routers on the network to learn consistent tables of next hop links which lead to relevant subnets.



Command Usage

- Just as Layer 2 switches use the Spanning Tree Algorithm to prevent loops, routers also use methods for preventing loops that would cause endless retransmission of data traffic. RIP utilizes the following three methods to prevent loops from occurring:
 - Split horizon – Never propagate routes back to an interface port from which they have been acquired.
 - Poison reverse – Propagate routes back to an interface port from which they have been acquired, but set the distance-vector metrics to infinity. (This provides faster convergence.)
 - Triggered updates – Whenever a route gets changed, broadcast an update message after waiting for a short random delay, but without waiting for the periodic cycle.
- RIP-2 is a compatible upgrade to RIP. RIP-2 adds useful capabilities for plain text authentication, multiple independent RIP domains, variable length subnet masks, and multicast transmissions for route advertising (RFC 1723).

- There are several serious problems with RIP that you should consider. First of all, RIP (version 1) has no knowledge of subnets, both RIP versions can take a long time to converge on a new route after the failure of a link or router during which time routing loops may occur, and its small hop count limitation of 15 restricts its use to smaller networks. Moreover, RIP (version 1) wastes valuable network bandwidth by propagating routing information via broadcasts; it also considers too few network variables to make the best routing decision.

Configuring General Protocol Settings

RIP is used to specify how routers exchange routing information. When RIP is enabled on this router, it sends RIP messages to all devices in the network every 30 seconds (by default), and updates its own routing table when RIP messages are received from other routers. To communicate properly with other routers using RIP, you need to specify the RIP version used globally by the router, as well as the RIP send and receive versions used on specific interfaces (page 3-179).

Command Usage

- When you specify a Global RIP Version, any VLAN interface not previously set to a specific Receive or Send Version (page 3-179) is set to the following values:
 - RIP Version 1 configures previously unset interfaces to send RIPv1 compatible protocol messages and receive either RIPv1 or RIPv2 protocol messages.
 - RIP Version 2 configures previously unset interfaces to use RIPv2 for both sending and receiving protocol messages.
- The *update* timer is the fundamental timer used to control all basic RIP processes.
 - Setting the update timer to a short interval can cause the router to spend an excessive amount of time processing updates. On the other hand, setting it to an excessively long time will make the routing protocol less sensitive to changes in the network configuration.
 - The timers must be set to the same values for all routers in the network.

Command Attributes

Global Settings

- **RIP Routing Process** – Enables RIP routing for all IP interfaces on the router. (Default: Disabled)
- **Global RIP Version** – Specifies a RIP version used globally by the router. (Default: RIP Version 1)

Timer Settings

- **Update** – Sets the rate at which updates are sent. This value will also set the timeout timer to 6 times the update time, and the garbage-collection timer to 4 times the update time. (Range: 15-60 seconds; Default: 30 seconds)
- **Timeout** – Sets the time after which there have been no update messages that a route is declared dead. The route is marked inaccessible (i.e., the metric set to infinite) and advertised as unreachable. However, packets are still forwarded on this route. (Default: 180 seconds)
- **Garbage Collection** – After the *timeout* interval expires, the router waits for an interval specified by the *garbage-collection* timer before removing this entry from the routing table. This timer allows neighbors to become aware of an invalid route prior to purging. (Default: 120 seconds)

Web - Click Routing Protocol, RIP, General Settings. Enable or disable RIP, set the RIP version used on previously unset interfaces to RIPv1 or RIPv2, set the basic update timer, and then click Apply.

General Settings	
Global	
RIP Routing Process	Enabled
Global RIP Version	RIPv2
Timer	
Update (15 - 60 seconds)	15
Timeout (Update x 6)	90
Garbage Collection (Update x 4)	60

CLI - This example sets the router to use RIP Version 2, and sets the basic timer to 15 seconds.

```
Console(config)#router rip                                4-231
Console(config-router)#version 2                          4-235
Console(config-router)#timers basic 15                    4-232
Console(config-router)#end
Console#show rip globals                                  4-242

RIP Process: Enabled
Update Time in Seconds: 15
Number of Route Change: 0
Number of Queries: 1
Console#
```

Specifying Network Interfaces for RIP

You must specify network interfaces that will be included in the RIP routing process.

Command Usage

- RIP only sends updates to interfaces specified by this command.
- Subnet addresses are interpreted as class A, B or C, based on the first field in the specified address. In other words, if a subnet address nnn.xxx.xxx.xxx is entered, the first field (nnn) determines the class:
 - 0 - 127 is class A, and only the first field in the network address is used.
 - 128 - 191 is class B, and the first two fields in the network address are used.
 - 192 - 223 is class C, and the first three fields in the network address are used.

Command Attributes

- **Subnet Address** – IP address of a network directly connected to this router.

Web - Click Routing Protocol, RIP, Network Addresses. Add all interfaces that will participate in RIP, and click Apply.

Network Addresses

Current:

- 10.1.0.0

<< Add Remove

New:

Subnet Address

CLI - This example includes network interface 10.1.0.0 in the RIP routing process.

```

Console(config)#router-rip                               4-231
Console(config-router)#network 10.1.0.0                  4-233
Console(config-router)#end
Console#show ip rip status                               4-242

```

Peer	UpdateTime	Version	RcvBadPackets	RcvBadRoutes
10.1.0.253		0	0	73
10.1.1.253		0	0	66

Console#

Configuring Network Interfaces for RIP

For each interface that participates in the RIP routing process, you must specify the protocol message type accepted (i.e., RIP version) and the message type sent (i.e., RIP version or compatibility mode), the method for preventing loopback of protocol messages, and whether or not authentication is used (i.e., authentication only applies if RIPv2 messages are being sent or received).

Command Usage

Specifying Receive and Send Protocol Types

- Setting the RIP Receive Version or Send Version for an interface overrides the global setting specified by the RIP / General Settings, Global RIP Version field.
- You can specify the Receive Version based on these options:
 - Use “RIPv1” or “RIPv2” if all routers in the local network are based on RIPv1 or RIPv2, respectively.
 - Use “RIPv1 or RIPv2” if some routers in the local network are using RIPv2, but there are still some older routers using RIPv1.
 - Use “Do Not Receive” if you do not want to add any dynamic entries to the routing table for an interface. (For example, you may only want to allow static routes for a specific interface.)
- You can specify the Send Version based on these options:
 - Use “RIPv1” or “RIPv2” if all routers in the local network are based on RIPv1 or RIPv2, respectively.
 - Use “RIPv1 Compatible” to propagate route information by broadcasting to other routers on the network using the RIPv2 advertisement list, instead of multicasting as normally required by RIPv2. (Using this mode allows RIPv1 routers to receive these protocol messages, but still allows RIPv2 routers to receive the additional information provided by RIPv2, including subnet mask, next hop and authentication information.)
 - Use “Do Not Send” to passively monitor route information advertised by other routers attached to the network.

Loopback Prevention

Just as Layer 2 switches use the Spanning Tree Algorithm to prevent loops, routers also use methods for preventing loops that would cause endless retransmission of data traffic. When protocol packets are caught in a loop, links will be congested, and protocol packets may be lost. However, the network will slowly converge to the new state. RIP utilizes the following

three methods that can provide faster convergence when the network topology changes and prevent most loops from occurring:

- **Split Horizon** – Never propagate routes back to an interface port from which they have been acquired.
- **Poison Reverse** – Propagate routes back to an interface port from which they have been acquired, but set the distance-vector metrics to infinity. (This provides faster convergence.)
- **Triggered Updates** – Whenever a route gets changed, broadcast an update message after waiting for a short random delay, but without waiting for the periodic cycle.

Protocol Message Authentication

RIPv1 is not a secure protocol. Any device sending protocol messages from UDP port 520 will be considered a router by its neighbors. Malicious or unwanted protocol messages can be easily propagated throughout the network if no authentication is required. RIPv2 supports authentication via a simple password. When a router is configured to exchange authentication messages, it will insert the password into all transmitted protocol packets, and check all received packets to ensure that they contain the authorized password. If any incoming protocol messages do not contain the correct password, they are simply dropped.

Command Attributes

- **VLAN** – ID of configured VLAN (1-4094).
- **Receive Version** – The RIP version to receive on an interface.
 - **RIPv1**: Accepts only RIPv1 packets.
 - **RIPv2**: Accepts only RIPv2 packets.
 - **RIPv1 or RIPv2**: Accepts RIPv1 or RIPv2 packets. (Default)
 - **Do Not Receive**: Does not accept incoming RIP packets.
 (The default depends on the setting specified under RIP / General Settings, Global RIP Version: RIPv1 - RIPv1 or RIPv2 packets, RIPv2 - RIPv2 packets)
- **Send Version** – The RIP version to send on an interface.
 - **RIPv1**: Sends only RIPv1 packets.

- **RIPv2:** Sends only RIPv2 packets.
- **RIPv1 Compatible:** Route information is broadcast to other routers with RIPv2. (Default)
- **Do Not Send:** Does not transmit RIP updates.
(The default depends on the setting specified under RIP / General Settings, Global RIP Version: RIPv1 - RIPv1 Compatible, RIPv2 - RIPv2 packets)
- **Instability Preventing** – Specifies the method used to reduce the convergence time when the network topology changes, and to prevent RIP protocol messages from looping back to the source router. (Default: Split Horizon)
 - **None:** No method is used. If a loop occurs, the hop count for a route may be gradually incremented to infinity (i.e., 16) before the route is deemed unreachable.
 - **Split Horizon:** This method never propagates routes back to an interface from which they have been acquired.
 - **Poision Reverse:** This method propagates routes back to an interface port from which they have been acquired, but set the distance-vector metrics to infinity. (This provides faster convergence.)
- **Authentication Type** – Specifies whether or not authentication is required for exchanging protocol messages. (Default: No Authentication)
 - **No Authentication:** No authentication is required.
 - **Simple Password:** Requires the interface to exchange routing information with other routers based on an authorized password.
(Note that authentication only applies to RIPv2.)
- **Authentication Key** – Specifies the key to use for authenticating RIPv2 packets. For authentication to function properly, both the sending and receiving interface must use the same password. (Range: 1-16 characters, case sensitive)

Web - Click Routing Protocol, RIP, Interface Settings. Select the RIP protocol message types that will be received and sent, the method used to provide faster convergence and prevent loopback (i.e., prevent instability in the network topology), and the authentication option and corresponding password. Then click Apply.

The screenshot shows a web interface titled "Interface Settings". It contains a table with the following fields and values:

VLAN	1
Receive Version	RIPv1 or RIPv2
Send Version	RIPv1 Compatible
Instability Preventing	Split Horizon
Authentication Type	SimplePassword
Authentication Key	mighty

CLI - This example sets the receive version to accept both RIPv1 or RIPv2 messages, the send mode to RIPv1 compatible (i.e., called v2-broadcast in the CLI), sets the method of preventing instability in the network topology to Split Horizon, enables authentication via a simple password (i.e., called text mode in the CLI).

```

Console(config)#interface vlan 1                                4-119
Console(config-if)#ip rip receive version 1 2                  4-236
Console(config-if)#ip rip send version v2-broadcast            4-237
Console(config-if)#ip split-horizon                            4-239
Console(config-if)#ip rip authentication mode text             4-241
Console(config-if)#ip rip authentication key mighty            4-240
Console#

```

Displaying RIP Information and Statistics

You can display basic information about the current global configuration settings for RIP, statistics about route changes and queries, information about the interfaces on this router that are using RIP, and information about known RIP peer devices.

RIP Information and Statistics

Parameter	Description
<i>Globals</i>	
RIP Routing Process	Indicates if RIP has been enabled or disabled.
Update Time in Seconds	The interval at which RIP advertises known route information. (Default: 30 seconds)
Number of Route Changes	Number of times routing information has changed.
Number of Queries	Number of router database queries received by this router.
<i>Interface Information</i>	
Interface	IP address of the interface.
SendMode	RIP version sent on this interface (none, RIPv1, RIPv2, rip1Compatible).
ReceiveMode	RIP version received on this interface (none, RIPv1, RIPv2, RIPv1Orv2).
InstabilityPreventing	Shows if split-horizon, poison-reverse, or no instability prevention method is in use.
AuthType	Shows if authentication is set to simple password or none.
RcvBadPackets	Number of bad RIP packets received.
RcvBadRoutes	Number of bad routes received.
SendUpdates	Number of route changes.
<i>Peer Information</i>	
PeerAddress	IP address of a neighboring RIP router.
UpdateTime	Last time a route update was received from this peer.
Version	Whether RIPv1 or RIPv2 packets were received from this peer.
RcvBadPackets	Number of bad RIP packets received from this peer.
RcvBadRoutes	Number of bad routes received from this peer.

Web - Click Routing Protocol, RIP, Statistics.

RIP Statistics

Globals

RIP Routing Process	Enabled
Update Time in Seconds	30
Number of Route Changes	4
Number of Queries	0

Interface Information

Interface	SendMode	ReceiveMode	InstabilityPreventing	AuthType	RcvBadPackets	RcvBadRoutes	SendUpdates
10.1.0.253, rip1Compatible, RIPv1Orv2, SplitHorizon, noAuthentication, 0, 0, 60							
10.1.1.253, rip1Compatible, RIPv1Orv2, SplitHorizon, noAuthentication, 0, 0, 60							

Peer Information

PeerAddress	UpdateTime	Version	RcvBadPackets	RcvBadRoutes
10.1.0.254, 4093, 2, 0, 14lu				
10.1.1.254, 4093, 2, 0, 14lu				

CLI - The information displayed by the RIP Statistics screen via the Web interface can be accessed from the CLI using the following commands.

Console#show rip globals4-242

RIP Process: Enabled

Update Time in Seconds: 30

Number of Route Change: 4

Number of Queries: 0

Console#show ip rip configuration4-242

Interface	SendMode	ReceiveMode	Poison	Authentication
10.1.0.253	rip1Compatible	RIPv1Orv2	SplitHorizon	noAuthentication
10.1.1.253	rip1Compatible	RIPv1Orv2	SplitHorizon	noAuthentication

Console#show ip rip status4-242

Interface	RcvBadPackets	RcvBadRoutes	SendUpdates
10.1.0.253	0	0	60
10.1.1.253	0	0	63

Console#show ip rip peer4-242

Peer	UpdateTime	Version	RcvBadPackets	RcvBadRoutes
10.1.0.254	4610	2	0	0
10.1.1.254	4610	2	0	0

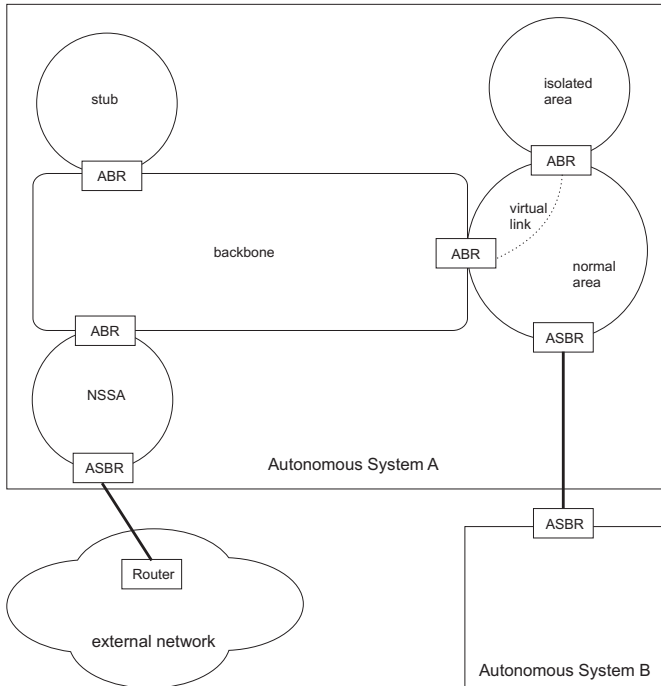
Console#

Configuring the Open Shortest Path First Protocol

Open Shortest Path First (OSPF) is more suited for large area networks which experience frequent changes in the links. It also handles subnets much better than RIP. OSPF protocol actively tests the status of each link to its neighbors to generate a shortest path tree, and builds a routing table based on this information. OSPF then utilizes IP multicast to propagate routing information. A separate routing area scheme is also used to further reduce the amount of routing traffic.

Note: The OSPF protocol implemented in this device is based on Version 2 (RFC 2328). It also supports Version 1 (RFC 1583) compatibility mode to ensure that the same method is used to calculate summary route costs throughout the network when older

OSPF routers exist; as well as the not-so-stubby area option (RFC 1587).



Command Usage

- OSPF looks at more than just the simple hop count. When adding the shortest path to any node into the tree, the optimal path is chosen on the basis of delay, throughput and connectivity. OSPF utilizes IP multicast to reduce the amount of routing traffic required when sending or receiving routing path updates. The separate routing area scheme used by OSPF further reduces the amount of routing traffic, and thus inherently provides another level of routing protection. In addition, all routing protocol exchanges can be authenticated. Finally, the OSPF algorithms have been tailored for efficient operation in TCP/IP Internets.

- OSPFv2 is a compatible upgrade to OSPF. It involves enhancements to protocol message authentication, and the addition of a point-to-multipoint interface which allows OSPF to run over non-broadcast networks, as well as support for overlapping area ranges.
- When using OSPF, you must organize your network (i.e., autonomous system) into normal, stub, or not-so-stubby areas; configure the ranges of subnet addresses that can be aggregated by link state advertisements; and configure virtual links for areas that do not have direct physical access to the OSPF backbone.
 - To implement OSPF for a large network, you must first organize the network into logical areas to limit the number of OSPF routers that actively exchange Link State Advertisements (LSAs). You can then define an OSPF interface by assigning an IP interface configured on this router to one of these areas. This OSPF interface will send and receive OSPF traffic to neighboring OSPF routers.
 - You can further optimize the exchange of OSPF traffic by specifying an area range that covers a large number of subnetwork addresses. This is an important technique for limiting the amount of traffic exchanged between Area Border Routers (ABRs).
 - And finally, you must specify a virtual link to any OSPF area that is not physically attached to the OSPF backbone. Virtual links can also be used to provide a redundant link between contiguous areas to prevent areas from being partitioned, or to merge backbone areas.

Configuring General Protocol Settings

To implement dynamic OSPF routing, first assign VLAN groups to each IP subnet to which this router will be attached, then use the OSPF / General Configuration menu to enable OSPF, assign an Router ID to this device, and set the other basic protocol parameters.

Command Attributes

General Information –

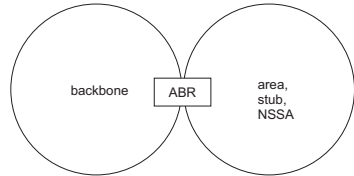
- **OSPF Routing Process** – Enables or disables OSPF routing for all IP interfaces on the router. (Default: Disabled)

- **OSPF Router ID** – Assigns a unique router ID for this device within the autonomous system. (Default: The lowest interface address)

- **Version Number**¹ – This router only supports OSPF Version 2.

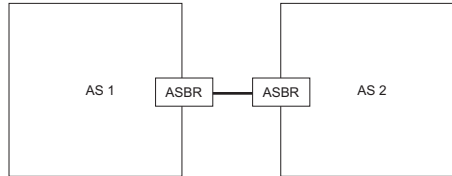
- **Area Border Router**¹ – Indicates if this router connect directly to networks in two or more areas.

An area border router runs a separate copy of the Shortest Path First algorithm, maintaining a separate routing database for each area.



- **AS Boundary Router**² –

Allows this router to exchange routing information with boundary routers in other autonomous systems to which it may be attached.



If a router is enabled as an ASBR, then every other router in the autonomous system can learn about external routes from this device. (Default: Disabled)

- **Rfc1583 Compatible** – If one or more routers in a routing domain are using OSPF Version 1, this router should use RFC 1583 (OSPFv1) compatibility mode to ensure that all routers are using the same RFC for calculating summary route costs. Enable this field to force the router to calculate summary route costs using RFC 1583. (Default: Disabled)
- **Auto Cost (Mbps)**¹ – This is the reference bandwidth used to calculate the default cost metric for each interface. To change the cost metric for any interface, use the OSP / Interface Configuration screen. (Default: 100)

1. These items are read only.

2. CLI - These items are configured with the **default-information originate** command (page -248).

- **SPF Hold Time (seconds)** – The hold time between making two consecutive shortest path first (SPF) calculations. (Range: 0-65535; Default: 10)
- **Area Numbers**¹ – The number of OSPF areas configured on this router.

Default Route Information –

- **Originate Default Route**² – Generates a default external route into an autonomous system. Note that the **AS Boundary Router** field must be enabled, and the **Advertise Default Route** field properly configured. (Default: Disabled)
- **Advertise Default Route**² – The router can advertise a default external route into the autonomous system (AS). (Options: NotAlways, Always; Default: NotAlways)
 - **Always** – The router will advertise itself as a default external route for the AS, even if a default external route does not actually exist.
 - **NotAlways** – It can only advertise a default external route into the AS if it has been configured to import external routes via RIP or static configuration, and such a route is known. (See “Redistributing External Routes” on page 210.)
- **External Metric Type**² – The external link type used to advertise the default route. Type 1 route advertisements add the internal cost to the external route metric. Type 2 routes do not add the internal cost metric. When comparing Type 2 routes, the internal cost is only used as a tie-breaker if several Type 2 routes have the same cost. (Default: Type 2)
- **Default External Metric**² – The Metric assigned to the default route. (Range: 1-65535; Default: 10)

1. These items are read only.

2. CLI - These items are configured with the **default-information originate** command (page -248).

Web - Click Routing Protocol, OSPF, General Configuration. Enable OSPF, specify the Router ID, configure the other global parameters as required, and click Apply.

General Configuration

General Information:

OSPF Routing Process	Enabled ▾
OSPF Router ID	10.1.1.253
Version Number	Version 2
Area Border Router	Yes
AS Boundary Router	Enabled ▾
RFC1583 Compatible	Disabled ▾
SPF Hold Time (0 - 65535 seconds)	10
Area Numbers	3

Default Information:

Originate Default Route	Enabled ▾
Advertise Default Route	Always ▾
External Metric Type	Type2 ▾
Default External Metric (0 - 16777215)	10

CLI - This example configures the router with the same settings as shown in the screen capture for the Web interface.

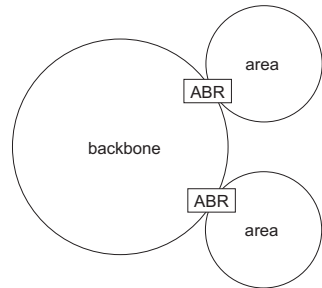
Console(config)#router ospf	4-246
Console(config-router)#router-id 10.1.1.253	4-247
Console(config-router)#no compatible rfc1583	4-248
Console(config-router)#default-information originate always	
metric 10 metric-type 2	4-248
Console(config-router)#timers spf 10	4-250
Console(config-router)#	

Configuring OSPF Areas

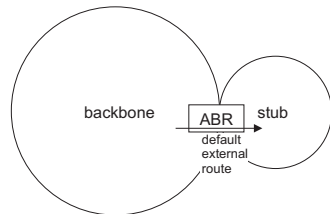
An autonomous system must be configured with a backbone area, designated by area identifier 0.0.0.0. By default, all other areas are created as normal transit areas.

Routers in a normal area may import or export routing information about individual nodes. To reduce the amount of routing traffic flooded onto the network, you can configure an area to export a single summarized route that covers a broad range of network addresses within the area (page 3-196). To further reduce the amount of routes passed between areas, you can configure an area as a stub or a not-so-stubby area (NSSA).

Normal Area – A large OSPF domain should be broken up into several areas to increase network stability and reduce the amount of routing traffic required through the use of route summaries that aggregate a range of addresses into a single route. The backbone or any normal area can pass traffic between other areas, and are therefore known as transit areas. Each router in an area has identical routing tables. These tables may include area links, summarized links, or external links that depict the topology of the autonomous system.



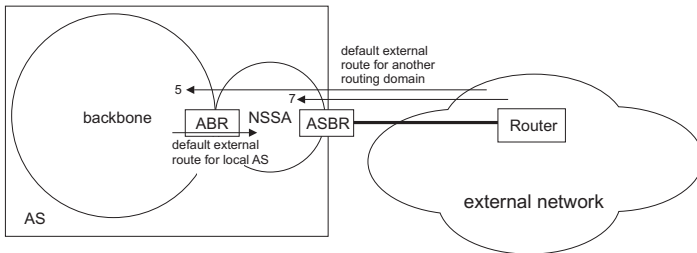
Stub – A stub does not accept external routing information. Instead, an area border router adjacent to a stub can be configured to send a default external route into the stub for all destinations outside the local area or the autonomous system. This route will also be



advertised as a single entry point for traffic entering the stub. Using a stub can significantly reduce the amount of topology data that has to be exchanged over the network.

- By default, a stub can only pass traffic to other areas in the autonomous system via the default external route. However, you also can configure an area border router to send Type 3 summary link advertisements into the stub.

NSSA – A not-so-stubby area (NSSA) is similar to a stub. It blocks most external routing information, and can be configured to advertise a single default route for traffic passing between the NSSA and other areas within the autonomous system (AS). However, an NSSA can also import external routes from one or more small routing domains that are not part of the AS, such as a RIP domain or locally configured static routes. This external AS routing information is generated by the NSSA's ASBR and advertised only within the NSSA. By default, these routes are not flooded onto the backbone or into any other area by area border routers. However, the NSSA's ABRs will convert NSSA external LSAs (Type 7) into external LSAs (Type-5) which are propagated into other areas within the AS.



- Routes that can be advertised with NSSA external LSAs include network destinations outside the AS learned via OSPF, the default route, static routes, routes derived from other routing protocols such as RIP, or directly connected networks that are not running OSPF.
- Also, note that unlike stub areas, all Type-3 summary LSAs are always imported into NSSAs to ensure that internal routes are always chosen over Type-7 NSSA external routes.

Default Cost – This specifies a cost for the default summary route sent into a stub or not-so-stubby area (NSSA) from an Area Border Router (ABR).

Command Usage

- Before you create a stub or NSSA, first specify the address range for an area using the Network Area Address Configuration screen (page 3-206).
- Stubs and NSSAs cannot be used as a transit area, and should therefore be placed at the edge of the routing domain.
- A stub or NSSA can have multiple ABRs or exit points. However, all of the exit points and local routers must contain the same external routing data so that the exit point does not need to be determined for each external destination.

Command Attributes

- **Area ID** – Identifier for an area, stub or NSSA.
- **Area Type** – Specifies a normal area, stub area, or not-so-stubby area (NSSA). Area ID 0.0.0.0 is set to the backbone by default.
(Default: Normal area)
- **Default Cost** – Cost for the default summary route sent into a stub from an area border router (ABR). (Range: 0-16777215; Default: 1)
 - Note that if you set the default cost to “0,” the router will not advertise a default route into the attached stub.
- **Summary** – Makes an ABR send a Type-3 summary link advertisement into a stub. (Default: Summary)
 - A stub is designed to save routing table space by blocking Type-4 AS summary LSAs and Type 5 external LSAs. If you use the “NoSummary” option to also block Type-3 summary LSAs that advertise the default route for destinations external to the local area or the AS, the stub will become completely isolated.

Note: This router supports up to 16 total areas (either normal transit areas, stubs, or NSSAs).

Web - Click Routing Protocol, OSPF, Area Configuration. Set any area to a stub or NSSA as required, specify the cost for the default summary route sent into a stub, and click Apply.

Area Configuration

Current Area Configuration:

Area ID	Area Type	Default Cost	Summary	Remove
0.0.0.0	Backbone			
0.0.0.1				<input type="checkbox"/>
0.0.0.2	Stub	10	Summary	<input type="checkbox"/>
0.0.0.3	NSSA			<input type="checkbox"/>

Entry Count: 4

Remove

Area Configuration Settings:

Area ID	<input type="text"/>
Area Type	Normal ▾
Default Cost (0 - 16777215)	<input type="text"/>
Summary	Summary ▾
<div>Set</div>	

CLI - This example configures area 0.0.0.1 as a normal area, area 0.0.0.2 as a stub, and area 0.0.0.3 as an NSSA. It also configures the router to propagate a default summary route into the stub and sets the cost for this default route to 10.

```

Console(config-router)#network 10.1.1.0 255.255.255.0
  area 0.0.0.1                                     4-255
Console(config-router)#area 0.0.0.2 stub summary   4-257
Console(config-router)#area 0.0.0.2 default-cost 10 4-252
Console(config-router)#area 0.0.0.3 nssa          4-258
Console(config-router)#end

```

```

Console#show ip ospf
Routing Process with ID 192.168.1.253
Supports only single TOS(TOS0) route
Number of area in this router is 3
Area 0.0.0.0 (BACKBONE)
    Number of interfaces in this area is 1
    SPF algorithm executed 40 times
Area 0.0.0.2 (STUB)
    Number of interfaces in this area is 1
    SPF algorithm executed 8 times
Area 0.0.0.3 (NSSA)
    Number of interfaces in this area is 1
    SPF algorithm executed 40 times
Console#

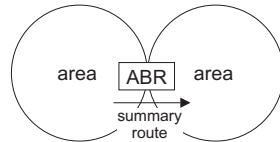
```

4-271

Configuring Area Ranges (Route Summarization for ABRs)

An OSPF area can include a large number of nodes. If the Area Border Router (ABR) has to advertise route information for each of these nodes, this wastes a lot of bandwidth and processor time. Instead, you can

configure an ABR to advertise a single summary route that covers all the individual networks within its area. When using route summaries, local changes do not have to be propagated to other area routers. This allows OSPF to be easily scaled for larger networks, and provides a more stable network topology.



Command Usage

- Use the Area Range Configuration page to summarize the routes for an area. The summary route for an area is defined by an IP address and network mask. You therefore need to structure each area with a contiguous set of addresses so that all routes in the area fall within an easily specified range. This router also supports Variable Length Subnet Masks (VLSMs), so you can summarize an address range on any bit boundary in a network address.
- To summarize the external LSAs imported into your autonomous system (i.e., local routing domain), use the Summary Address Configuration screen (page 3-208).

Command Attributes

- **Area ID** – Identifies an area for which the routes are summarized.
(The area ID must be in the form of an IP address.)
- **Range Network** – Base address for the routes to summarize.
- **Range Netmask** – Network mask for the summary route.
- **Advertising** – Indicates whether or not to advertise the summary route.
If the summary is not sent, the routes remain hidden from the rest of the network. (Default: Advertise)

Note: This router supports up to 64 summary routes for area ranges.

Web - Click Routing Protocol, OSPF, Area Range Configuration. Specify the area identifier, the base address and network mask, select whether or not to advertise the summary route to other areas, and then click Apply.

Area Range Configuration

Current Area Range Entries:

Area ID	Range Network	Range Netmask	Advertising	Remove
0.0.0.1	10.1.1.0	255.255.255.0	Advertise ▼	<input type="checkbox"/>

Entry Count: 1

Area Range Settings:

Area ID	<input type="text"/>	Range Network	<input type="text"/>
Advertising	Advertise ▼	Range Netmask	<input type="text"/>

CLI - This example summarizes all the routes for area 1. Note that the default for the **area range** command is to advertise the route summary. The configured summary route is shown in the list of information displayed for area 1.

```
Console(config-router)#area 0.0.0.1 range 10.1.1.0
255.255.255.0
Console(config-router)#end
Console#show ip ospf
Routing Process with ID 10.1.1.253
Supports only single TOS(TOS0) route
Number of area in this router is 4
Area 0.0.0.0 (BACKBONE)
    Number of interfaces in this area is 0
    SPF algorithm executed 47 times
Area 0.0.0.1
    Number of interfaces in this area is 3
    SPF algorithm executed 14 times
    Area ranges are
        255.255.255.0/24   Active
Console#
```

Configuring OSPF Interfaces

You should specify a routing interface for any local subnet that needs to communicate with other network segments located on this router or elsewhere in the network. First configure a VLAN for each subnet that will be directly connected to this router, assign IP interfaces to each VLAN (i.e., one primary interface and one or more secondary interfaces), and then use the OSPF / Network Area Address Configuration page to assign an interface address range to an OSPF area.

After assigning a routing interface to an OSPF area, you need to use the OSPF / Interface Configuration page to configure the interface-specific parameters used by OSPF to select the designated router, control the timing of link state advertisements, set the cost used to select preferred paths, and specify the method used to authenticate routing messages.

Field Attributes*OSPF Interface List*

- **VLAN ID** – The VLAN to which an IP interface has been assigned.
- **Interface IP** – The IP interface associated with the selected VLAN.
- **Area ID** – The area to which this interface has been assigned.
- **Designated Router** – Designated router for this area.
- **Backup Designated Router** – Designated backup router for this area.
- **Entry Count** – The number of IP interfaces assigned to this VLAN.

Note: This router supports up to 64 OSPF interfaces.

Detail Interface Configuration

- **VLAN ID** – The VLAN corresponding to the selected interface.
- **Rtr Priority** – Sets the interface priority for this router.
(Range: 0-255; Default: 1)
 - A designated router (DR) and backup designated router (BDR) is elected for each OSPF area based on Router Priority. The DR forms an active adjacency to all other routers in the area to exchange routing topology information. If for any reason the DR fails, the BDR takes over this role.
 - The router with the highest priority becomes the DR and the router with the next highest priority becomes the BDR. If two or more routers are set to the same priority, the router with the higher ID will be elected. You can set the priority to zero to prevent a router from being elected as a DR or BDR.
 - If a DR already exists for an area when this interface comes up, the new router will accept the current DR regardless of its own priority. The DR will not change until the next time the election process is initiated.
- **Transmit Delay** – Sets the estimated time to send a link-state update packet over an interface. (Range: 1-65535 seconds; Default: 1)
 - LSAs have their age incremented by a delay before transmission. You should consider both the transmission and propagation delays for an

- interface when estimating this delay. Set the transmit delay according to link speed, using larger values for lower-speed links.
- The transmit delay must be the same for all routers in an autonomous system.
 - On slow links, the router may send packets more quickly than devices can receive them. To avoid this problem, you can use the transmit delay to force the router to wait a specified interval between transmissions.
- **Retransmit Interval** – Sets the time between resending link-state advertisements. (Range: 1-65535 seconds; Default: 1)
 - A router will resend an LSA to a neighbor if it receives no acknowledgment. The retransmit interval should be set to a conservative value that provides an adequate flow of routing information, but does not produce unnecessary protocol traffic. Note that this value should be larger for virtual links.
 - Set this interval to a value that is greater than the round-trip delay between any two routers on the attached network to avoid unnecessary retransmissions.
 - **Hello Interval** – Sets the interval between sending hello packets on an interface. (Range: 1-65535 seconds; Default: 10)
 - This interval must be set to the same value for all routers on the network.
 - Using a smaller Hello interval allows changes in the network topology to be discovered more quickly, but may result in more routing traffic.
 - **Rtr Dead Interval** – Sets the interval at which hello packets are not seen before neighbors declare the router down. This interval must be set to the same value for all routers on the network. (Range: 1-65535 seconds; Default: 40, or 4 times the Hello Interval)
 - **Cost** – Sets the cost of sending a packet on an interface, where higher values indicate slower ports. (Range: 1-65535; Default: 1)
 - This router uses a default cost of 1 for all ports. Therefore, if you install a Gigabit module, you need to reset the cost for all of the 100 Mbps ports to some value greater than 1.
 - Routes are subsequently assigned a metric equal to the sum of all metrics for each interface link in the route.

- **Authentication Type** – Specifies the authentication type used for an interface. (Options: None, Simple password, MD5; Default: None)
 - Use authentication to prevent routers from inadvertently joining an unauthorized area. Configure routers in the same area with the same password or key.
 - When using simple password authentication, a password is included in the packet. If it does not match the password configured on the receiving router, the packet is discarded. This method provides very little security as it is possible to learn the authentication key by snooping on routing protocol packets.
 - When using Message-Digest 5 (MD5) authentication, the router uses the MD5 algorithm to verify data integrity by creating a 128-bit message digest from the authentication key. Without the proper key and key-id, it is nearly impossible to produce any message that matches the prespecified target message digest.
 - The Authentication Key and Message Digest Key-id must be used consistently throughout the autonomous system. (Note that the Message Digest Key-id field is disabled when this authentication type is selected.)
- **Authentication Key** – Assign a plain-text password used by neighboring routers to verify the authenticity of routing protocol messages. (Range: 1-8 characters for simple password or 1-16 characters for MD5 authentication; Default: no key)
 - You can assign a unique password to each network (i.e., autonomous system) to improve the security of the routing database. However, the password must be used consistently on all neighboring routers throughout a network.
- **Message Digest Key-id** – Assigns a key-id used in conjunction with the authentication key to verify the authenticity of routing protocol messages sent to neighboring routers. (Range: 1-255; Default: none)
 - Normally, only one key is used per interface to generate authentication information for outbound packets and to authenticate incoming packets. Neighbor routers must use the same key identifier and key value.

- When changing to a new key, the router will send multiple copies of all protocol messages, one with the old key and another with the new key. Once all the neighboring routers start sending protocol messages back to this router with the new key, the router will stop using the old key. This rollover process gives the network administrator time to update all the routers on the network without affecting the network connectivity. Once all the network routers have been updated with the new key, the old key should be removed for security reasons.

Web - Click Routing Protocol, OSPF, Interface Configuration. Select the required interface from the scroll-down box, and click Detailed Settings

Interface Configuration

OSPF Interface List of **VLAN ID :** 1 Detail Setting

Interface IP	Area ID	Designated Router	Backup DesignatedRouter
10.1.1.252	0.0.0.0	10.1.1.253	10.1.1.252

Entry Count: 1

Change any of the interface-specific protocol parameters, and then click Apply

Detailed Interface Configuration	
VLAN ID	1
Rtr Priority (0 - 255)	5
Transmit Delay (0 - 3600 seconds)	6
Retransmit Interval (0 - 3600 seconds)	7
Hello Interval (1 - 65535 seconds)	5
Rtr Dead Interval (0 - 65535 seconds)	50
Cost (0 - 65535)	10
Authentication Type	MD 5
Authentication Key	aiebel
Message Digest Key-id (0 - 255)	1

CLI - This example configures the interface parameters for VLAN 1.

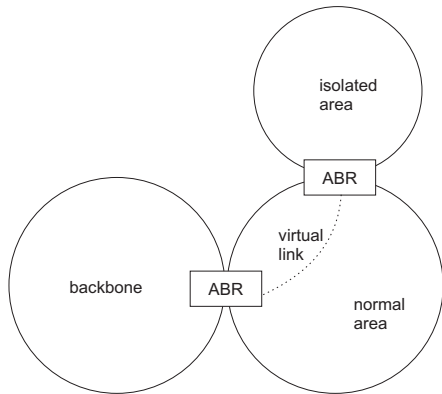
```

Console(config)#interface vlan 1
Console(config-if)#ip ospf priority 5                                4-268
Console(config-if)#ip ospf transmit-delay 6                          4-270
Console(config-if)#ip ospf retransmit-interval 7                     4-269
Console(config-if)#ip ospf hello-interval 5                         4-268
Console(config-if)#ip ospf dead-interval 50                         4-267
Console(config-if)#ip ospf cost 10                                  4-266
Console(config-if)#ip ospf authentication message-digest            4-263
Console(config-if)#ip ospf message-digest-key 1 md5 aiebel          4-265
Console#

```

Configuring Virtual Links

All OSPF areas must connect to the backbone. If an area does not have a direct physical connection to the backbone, you can configure a virtual link that provides a logical path to the backbone. To connect an isolated area to the backbone, the logical path can cross a single non-backbone area (i.e.,



transit area) to reach the backbone. To define this path, you must configure an ABR that serves as an endpoint connecting the isolated area to the common transit area, and specify a neighboring ABR as the other endpoint connecting the common transit area to the backbone itself. (Note that you cannot configure a virtual link that runs through a stub or NSSA area.)

Virtual links can also be used to create a redundant link between any area and the backbone to help prevent partitioning, or to connect two existing backbone areas into a common backbone.

Command Attributes

- **Area ID** – Identifies the transit area for the virtual link. (The area ID must be in the form of an IP address.)
- **Neighbor Router ID** – Neighbor router at other end of the virtual link. This must be an Area Border Router (ABR) that is adjacent to both the backbone and the transit area for the virtual link.
- **Events** – The number of state changes or error events on this virtual link.

The other items are described under “Configuring OSPF Interfaces,” page 3-198.

Note: This router supports up to 64 virtual links.

Web - Click Routing Protocol, OSPF, Virtual Link Configuration. To create a new virtual link, specify the Area ID and Neighbor Router ID, configure the link attributes, and click Add. To modify the settings for an existing link, click the Detail button for the required entry, modify the link settings, and click Set.

Virtual Link Configuration

Current Virtual Link Entries:

Area ID	Neighbor Router ID	Detail Setting	Remove
0.0.0.4	10.1.1.252	<input type="button" value="Detail"/>	<input type="checkbox"/>

Entry Count: 1

Virtual Link Settings:

Area ID	<input type="text"/>
Neighbor Router ID	<input type="text"/>
Transmit Delay (0 - 3600 seconds)	<input type="text" value="1"/>
Retransmit Interval (0 - 3600 seconds)	<input type="text" value="5"/>
Hello Interval (1 - 65535 seconds)	<input type="text" value="10"/>
Rtr Dead Interval (0 - 65535 seconds)	<input type="text" value="40"/>
Authentication Type	<input type="text" value="Null"/>
Authentication Key	<input type="text"/>
Message Digest Key-id (0 - 255)	<input type="text"/>
<input type="button" value="Add"/>	

CLI - This example configures a virtual link from the ABR adjacent to area 0.0.0.4, through a transit area to the neighbor router 10.1.1.252 at the other end of the link which is adjacent to the backbone.

```
Console(config-router)#area 0.0.0.0 virtual-link 10.1.1.252 4-260
Console(config-router)#
```

Configuring Network Area Addresses

OSPF protocol broadcast messages (i.e., Link State Advertisements or LSAs) are restricted by area to limit their impact on network performance. A large network should be split up into separate OSPF areas to increase network stability, and to reduce protocol traffic by summarizing routing information into more compact messages. Each router in an area shares the same view of the network topology, including area links, route summaries for directly connected areas, and external links to other areas.

Command Usage

- Use the Network Area Address Configuration page to specify an Area ID and the corresponding network address range. Each area identifies a logical group of OSPF routers that actively exchange LSAs to ensure that they share an identical view of the network topology.
- Each area must be connected to a backbone area. This area passes routing information between other areas in the autonomous system. The default value 0.0.0.0 is used as the Area ID for the backbone. All routers must be connected to the backbone, either directly, or through a virtual link if a direct physical connection is not possible.
- An area initially configured via the Network Area Address Configuration page is set as a normal area (or transit area) by default. A normal area can send and receive external Link State Advertisements (LSAs). If necessary, you can use the Area Configuration page to configure an area as a stubby area that cannot send or receive external LSAs, or a not-so-stubby area (NSSA) that can import external route information into its area (page 3-192).
- An area must be assigned a range of subnetwork addresses. This area and the corresponding address range forms a routing interface, and can be configured to aggregate LSAs from all of its subnetwork addresses and exchange this information with other routers in the network (page 3-196).

Command Attributes

- **IP Address** – Address of the interfaces to add to the area.
- **Netmask** – Network mask of the address range to add to the area.
- **Area ID** – Area to which the specified address or range is assigned. An OSPF area identifies a group of routers that share common routing information. (The area ID must be in the form of an IP address.)

Note: This router supports up to 16 total areas (either normal transit areas, stubs, or NSSAs).

Web - Click Routing Protocol, OSPF, Network Area Address Configuration. Configure a backbone area that is contiguous with all the other areas in your network, configure an area for all of the other OSPF interfaces, then click Apply.

Network Area Address Configuration

Current Network Address Entries:

IP Address	Netmask	Area ID	Remove
10.0.0.0	255.0.0.0	0.0.0.0	<input type="checkbox"/>
10.1.1.0	255.255.255.0	0.0.0.1	<input type="checkbox"/>
10.1.2.0	255.255.255.0	0.0.0.2	<input type="checkbox"/>
10.1.3.0	255.255.255.0	0.0.0.3	<input type="checkbox"/>

Entry Count: 4

Network Address Settings:

IP Address	<input style="width: 80%;" type="text"/>
Netmask	<input style="width: 80%;" type="text"/>
Area ID	<input style="width: 80%;" type="text"/>
<input type="button" value="Set"/>	

CLI - This example configures the backbone area and one transit area.

```
Console(config-router)#network 10.0.0.0 255.0.0.0
    area 0.0.0.0
Console(config-router)#network 10.1.1.0 255.255.255.0 area 0.0.0.1
Console(config-router)#end
Console#show ip ospf
Routing Process with ID 10.1.1.253
Supports only single TOS(TOS0) route
Number of area in this router is 4
Area 0.0.0.0 (BACKBONE)
    Number of interfaces in this area is 1
    SPF algorithm executed 8 times
Area 0.0.0.1
    Number of interfaces in this area is 1
    SPF algorithm executed 5 times
Area 0.0.0.2 (STUB)
    Number of interfaces in this area is 1
    SPF algorithm executed 13 times
Area 0.0.0.3 (NSSA)
    Number of interfaces in this area is 1
    SPF algorithm executed 12 times
Console#
```

Configuring Summary Addresses (for External AS Routes)

An Autonomous System Boundary Router (ASBR) can redistribute routes learned from other protocols into all attached autonomous systems. (See “Redistributing External Routes” on page 3-210) To reduce the amount of external LSAs imported into your local routing domain, you can configure the router to advertise an aggregate route that consolidates a broad range of external addresses.

Command Usage

- If you are not sure what address ranges to consolidate, first enable external route redistribution via the Redistribute Configuration screen, view the routes imported into the routing table, and then configure one or more summary addresses to reduce the size of the routing table and consolidate these external routes for advertising into the local domain.
- To summarize routes sent between OSPF areas, use the Area Range Configuration screen (page 3-196).

Command Attributes

- **IP Address** – Summary address covering a range of addresses.
- **Netmask** – Network mask for the summary route.

Note: This router supports up to 16 Type-5 summary routes.

Web - Click Routing Protocol, OSPF, Summary Address Configuration. Specify the base address and network mask, then click Add.

Summary Address Configuration

Current Summary Address Entries:

IP Address	Netmask	Remove
10.1.0.0	255.255.0.0	<input type="checkbox"/>

Entry Count: 1
Remove

Summary Address Settings:

IP Address

Netmask

Add

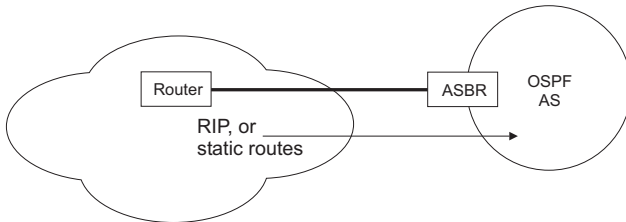
CLI - This example This example creates a summary address for all routes contained in 192.168.x.x.

```
Console(config-router)#summary-address 192.168.0.0
255.255.0.0
Console(config-router)#
```

4-253

Redistributing External Routes

You can configure this router to import external routing information from other routing protocols into the autonomous system.



Command Usage

- This router supports redistribution for both RIP and static routes.
- When you redistribute external routes into an OSPF autonomous system (AS), the router automatically becomes an autonomous system boundary router (ASBR).
- However, if the router has been manually configured as an ASBR via the General Configuration screen, but redistribution is not enabled, the router will only generate a “default” external route into the AS if it has been configured to “always” advertise a default route even if an external route does not actually exist (page 3-188).
- Metric type specifies the way to advertise routes to destinations outside the autonomous system (AS) via External LSAs. Specify Type 1 to add the internal cost metric to the external route metric. In other words, the cost of the route from any router within the AS is equal to the cost associated with reaching the advertising ASBR, plus the cost of the external route. Specify Type 2 to only advertise external route metric.
- The metric value specified for redistributed routes supersedes the Default External Metric specified in the OSPF / General Configuration screen (page 3-188).

Command Attributes

- **Redistribute Protocol** – Specifies the external routing protocol type for which routing information is to be redistributed into the local routing domain. (Options: RIP, Static; Default: RIP)
- **Redistribute Metric Type** – Indicates the method used to calculate external route costs. (Options: Type 1, Type 2; Default: Type 1)
- **Redistribute Metric** – Metric assigned to all external routes for the specified protocol. (Range: 1-65535; Default: 10)

Web - Click Routing Protocol, OSPF, Redistribute Configuration. Specify the protocol type to import, the metric type and path cost, then click Add.

Redistribute Configuration

Current Redistribute Protocol:

Redistribute Protocol	Redistribute Metric Type	Redistribute Metric	Remove
RIP	Type1	10	<input type="checkbox"/>
Entry Count: 1			<input type="button" value="Remove"/>

Redistribute Settings:

Redistribute Protocol	<input type="text" value="RIP"/>
Redistribute Metric Type	<input type="text" value="Type1"/>
Redistribute Metric (0 - 16777215)	<input type="text" value="10"/>
<input type="button" value="Set"/>	

CLI - This example redistributes routes learned from RIP as Type 1 external routes.

```
Console(config-router)#redistribute rip metric-type 1
Console(config-router)#
```

4-254

Configuring NSSA Settings

Use the OSPF / NSSA Settings page to configure a not-so-stubby area (NSSA), and to control the use of default routes for ABRs and ASBRs, or external routes learned from other routing domains and imported via an ABR. (For a detailed description of NSSA areas, refer to “Configuring OSPF Areas” on page 3-192.)

Command Attributes

- **Area ID** – Identifier for an not-so-stubby area (NSSA).
- **Default Information Originate** – An NSSA ASBR originates and floods Type-7 external LSAs throughout its area for known network destination outside of the AS. However, you can also configure an NSSA ASBR to generate a Type-7 “default” route to areas outside of the AS, or an NSSA ABR to generate a Type-7 “default” route to other areas within the AS. (Default: Disabled)
- **No Redistribution** – The Redistribute Configuration page (page 3-210) is used to import information from other routing domains (or protocols) into the AS. However, when the router is an NSSA ABR, you can choose whether or not to accept external routes learned from routers in other OSPF areas into the NSSA. (Default: Enabled)

Note: This router supports up 16 areas, either normal transit areas, stubs, or NSSAs.

Web - Click Routing Protocol, OSPF, NSSA Settings. Create a new NSSA or modify the routing behavior for an existing NSSA, and click Apply.

NSSA Settings

Current NSSA Settings:

Area ID	Default Information Originate	No Redistribution	Remove
0.0.0.1	Enabled ▾	Disabled ▾	<input type="checkbox"/>
0.0.0.2	Disabled ▾	Enabled ▾	<input type="checkbox"/>

Entry Count: 3
Remove

NSSA Settings:

Area ID	<input style="width: 100%;" type="text"/>
Default Information Originate	Enabled ▾
No Redistribution	Enabled ▾
Set	

CLI - This example configures area 0.0.0.1 as a stub and sets the cost for the default summary route to 10.

```

Console(config-router)#area 0.0.0.1 nssa
default-information-originate                               4-258
Console(config-router)#area 0.0.0.2 nssa no-redistribution  4-258
Console(config-router)#
  
```

Displaying Link State Database Information

OSPF routers advertise routes using Link State Advertisements (LSAs). The full collection of LSAs collected by a router interface from the attached area is known as a link state database. Routers that are connected to multiple interfaces will have a separate database for each area. Each router in the same area should have an identical database describing the topology for that area, and the shortest path to external destinations.

The full database is exchanged between neighboring routers as soon as a new router is discovered. Afterwards, any changes that occur in the routing tables are synchronized with neighboring routers through a process called reliable flooding. You can show information about different LSAs stored in this router's database, which may include any of the following types:

- Router (Type 1) – All routers in an OSPF area originate Router LSAs that describe the state and cost of its active interfaces and neighbors.
- Network (Type 2) – The designated router for each area originates a Network LSA that describes all the routers that are attached to this network segment.
- Summary (Type 3) – Area border routers can generate Summary LSAs that give the cost to a subnetwork located outside the area.
- AS Summary (Type 4) – Area border routers can generate AS Summary LSAs that give the cost to an autonomous system boundary router (ASBR).
- AS External (Type 5) – An ASBR can generate an AS External LSA for each known network destination outside the AS.
- NSSA External (Type 7) – An ASBR within an NSSA generates an NSSA external link state advertisement for each known network destination outside the AS.

Command Attributes

- **Area ID** – Area defined for which you want to view LSA information. (This item must be entered in the form of an IP address.)
- **Link ID** – The network portion described by an LSA. The Link ID should be:
 - An IP network number for Type 3 Summary and Type 5 AS External LSAs. (When an Type 5 AS External LSA is describing a default route, its Link ID is set to the default destination 0.0.0.0.)
 - A Router ID for Router, Network, and Type 4 AS Summary LSAs.
- **Self-Originate** – Shows LSAs originated by this router.
- **LS Type** – LSA Type (Options: Type 1-5, 7). See the preceding description.

- **Adv Router** – IP address of the advertising router. If not entered, information about all advertising routers is displayed.
- **Age*** – Age of LSA (in seconds).
- **Seq*** – Sequence number of LSA (used to detect older duplicate LSAs).
- **Checksum*** – Checksum of the complete contents of the LSA.

* These items are read only.

Web - Click Routing Protocol, OSPF, Link State Database Information. Specify parameters for the LSAs you want to display, then click Query.

Link State Database Information

Query by:

☐ Area ID

☐ Link ID

☐ Self-Originate

☐ LS Type

☐ ADV Router

Query By : "none"

Search Results : 22 results (Total)
Type 1 : RouterLink (1) Type 2 : NetworkLink (2) Type 3 : SummaryLink (3)
Type 4 : asSummaryLink (4) Type 5 : asExternalLink (5) Type 7 : NSSAExternalLink (7)

Link State Data Router (Type 1)

Area ID	Link ID	ADV Router	Age	Seq#	Checksum
0.0.0.1	10.2.45.188	10.2.44.50	1002	0x8000001B	0xDCB7

CLI - The CLI provides a wider selection of display options for viewing the Link State Database. See “show ip ospf database” on page -273.

Displaying Information on Border Routers

You can display entries in the local routing table for Area Border Routers (ABR) and Autonomous System Boundary Routers (ASBR) known by this device.

Field Attributes

- **Destination** – Identifier for the destination router.
- **Next Hop** – IP address of the next hop toward the destination.
- **Cost** – Link metric for this route.
- **Type** – Router type of the destination; either ABR, ASBR or both.
- **Rte Type** – Route type; either intra-area or interarea route (INTRA or INTER).
- **Area** – The area from which this route was learned.
- **SPF No** – The number of times the shortest path first algorithm has been executed for this route.

Web - Click Routing Protocol, OSPF, Border Router Information.

Border Router Information						
Destination	Next Hop	Cost	Type	RteType	Area ID	SPF No
10.2.44.5	10.2.44.88	1	ABR	INTRA	0.0.0.1	5
10.2.44.5	10.2.44.88	1	ASBR	INTER	0.0.0.1	5

Entry Count: 2

CLI - This example shows one router that serves as both the ABR for the local area and the ASBR for the autonomous system.

Console#show ip ospf border-routers							4-272
Destination	Next Hop	Cost	Type	RteType	Area	SPF No	
10.2.44.5	10.2.44.88	1	ABR	INTRA	0.0.0.1	5	
10.2.44.5	10.2.44.88	1	ASBR	INTER	0.0.0.1	5	

Console#

Displaying Information on Neighbor Routers

You can display about neighboring routers on each interface within an OSPF area.

Field Attributes

- **ID** – Neighbor's router ID.
- **Priority** – Neighbor's router priority.
- **State** – OSPF state and identification flag.

States include:

- Down – Connection down
- Attempt – Connection down, but attempting contact (non-broadcast networks)
- Init – Have received Hello packet, but communications not yet established
- Two-way – Bidirectional communications established
- ExStart – Initializing adjacency between neighbors
- Exchange – Database descriptions being exchanged
- Loading – LSA databases being exchanged
- Full – Neighboring routers now fully adjacent

Identification flags include:

- D – Dynamic neighbor
 - S – Static neighbor
 - DR – Designated router
 - BDR – Backup designated router
- **Address** – IP address of this interface.

Web - Click Routing Protocol, OSPF, Neighbor Information.

Neighbor Information			
ID	Priority	State	Address
10.2.44.5	1	FULL/DR	10.2.44.88
10.2.44.5	2	FULL/BDR	10.2.44.88

Entry Count: 2

CLI - This shows a designated router and backup designated router as neighbors.

Console#show ip ospf neighbor				4-282
ID	Pri	State	Address	
10.2.44.5	1	FULL/DR	10.2.44.88	
10.2.44.6	2	FULL/BDR	10.2.44.88	
Console#				

Multicast Routing

This router can route multicast traffic to different subnetworks using either Distance Vector Multicast Routing Protocol (DVMRP) or Protocol-Independent Multicasting - Dense Mode (PIM-DM). These protocols flood multicast traffic downstream, and calculate the shortest-path, source-rooted delivery tree between each source and destination host group. They also rely on messages sent from IGMP-enabled Layer 2 switches and hosts to determine when hosts want to join or leave multicast groups.

DVMRP builds a source-rooted multicast delivery tree that allows it to prevent looping and determine the shortest path to the source of the multicast traffic. PIM also builds a source-rooted multicast delivery tree for each multicast source, but uses information from the router's unicast routing table instead of maintaining its own multicast routing table, making

it routing protocol independent. Also note that the Dense Mode version of PIM is supported on this router because it is suitable for densely populated multicast groups which occur primarily in the LAN environment.

If DVMRP and PIM-DM are not enabled on this router or another multicast routing protocol is used on your network, you can manually configure the switch ports attached to a multicast router (page 3-140).

Configuring Global Settings for Multicast Routing

To use multicast routing on this router, you must first globally enable multicast routing as described in this section, globally enable DVRMP (page 3-223) or PIM (page 3-232), and specify the interfaces that will participate (page 3-227 or 3-233). Note that you can only enable one multicast routing protocol on any given interface.

Web – Click IP, Multicast Routing, General Setting, Set Multicast Forwarding Status to Enabled, and click Apply.

Multicast Routing General Setting

Multicast Forwarding Status

Enabled ▼

CLI – This example enables multicast routing globally for the router.

```
Console(config)#ip multicast-routing
Console(config)#
```

4-288

Displaying the Multicast Routing Table

You can display information on each multicast route this router has learned via DVMRP or PIM. The router learns multicast routes from neighboring routers, and also advertises these routes to its neighbors. The router stores entries for all paths learned by itself or from other routers, without considering actual group membership or prune messages. The routing table therefore does not indicate that the router has processed multicast traffic from any particular source listed in the table. It uses these

routes to forward multicast traffic only if group members appear on directly-attached subnetworks or on subnetworks attached to downstream routers.

Field Attributes

- **Group Address** – IP group address for a multicast service.
- **Source Address** – Subnetwork containing the IP multicast source.
- **Netmask** – Network mask for the IP multicast source.
- **Interface** – Interface leading to the upstream neighbor.
- **Owner** – The associated multicast protocol (i.e., DVMRP or PIM).
- **Flags** – The flags associated with each interface indicate prune (P) if the downstream interface has been recently terminated or forwarding (F) if the interface is still active.
- **Detail** – This button displays detailed information for the selected entry.
- **Upstream Router*** – The multicast router immediately upstream for this group.
- **Downstream*** – Interface(s) on which multicast subscribers have been recorded.

* These items are displayed in the IP Multicast Routing Entry (Detail) table.

Web – Click IP, Multicast Routing, Multicast Routing Table. Click Detail to display additional information for any entry.

IP Multicast Routing Table (Summary)

Flags: P - Prune Up

Group Address	Source Address	Netmask	Interface	Owner	Flags	Detail
234.5.6.7	10.1.0.0	255.255.255.0	VLAN2	DVMRP	--	Detail
234.5.6.8	10.1.5.19	255.255.255.255	VLAN3	PIM-DM	--	Detail

Entry Count: 2

IP Multicast Routing Entry (Detail)

IP Multicast Routing Table
Flags: P | ✓ Prune, F - Forwarding

Source Address:	10.1.0.0
Netmask:	255.255.255.0
Group Address:	234.5.6.7
Owner:	DVMRP
Upstream Interface:	VLAN 2
Upstream Router:	10.1.0.0
Downstream:	(none)

CLI – This example shows that multicast forwarding is enabled. The multicast routing table displays one entry for a multicast source routed by DVMRP, and another source routed via PIM.

```
Console#show ip mroute 4-288
IP Multicast Forwarding is enabled.

IP Multicast Routing Table

Flags:  P - Prune, F - Forwarding

(234.5.6.7, 10.1.0.0, 255.255.255.0)
Owner: DVMRP
Upstream Interface: vlan2
Upstream Router: 10.1.0.0
Downstream:

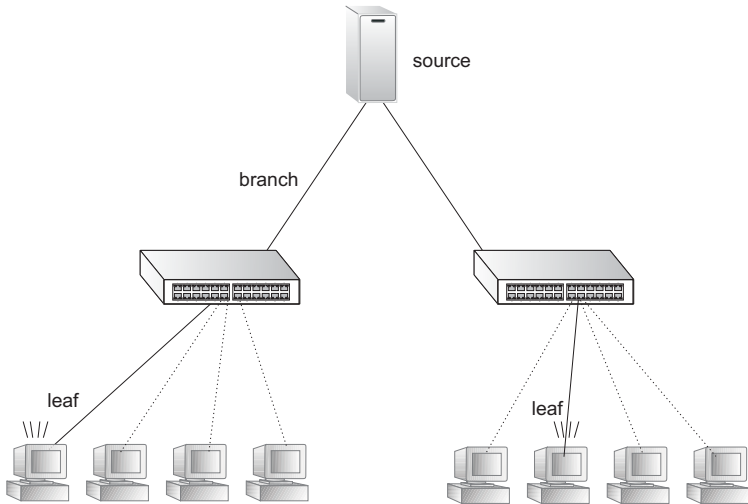
(234.5.6.8, 10.1.5.19, 255.255.255.255)
Owner: PIM-DM
Upstream Interface: vlan3
Upstream Router: 10.1.5.19
Downstream:

Console#
```

Configuring DVMRP

The Distance-Vector Multicast Routing Protocol (DVMRP) behaves somewhat similarly to RIP. A router supporting DVMRP periodically floods its attached networks to pass information about supported multicast services along to new routers and hosts. Routers that receive a DVMRP packet send a copy out to all paths (except the path back to the origin). These routers then send a prune message back to the source to stop a data stream if the router is attached to a LAN which does not want to receive traffic from a particular multicast group. However, if a host attached to this router issues an IGMP message indicating that it wants to subscribe to the concerned multicast service, this router will use DVMRP

to build up a source-rooted multicast delivery tree that allows it to prevent looping and determine the shortest path to the source of this multicast traffic.



When this router receives the multicast message, it checks its unicast routing table to locate the port that provides the shortest path back to the source. If that path passes through the same port on which the multicast message was received, then this router records path information for the concerned multicast group in its routing table and forwards the multicast message on to adjacent routers, except for the port through which the message arrived. This process eliminates potential loops from the tree and ensures that the shortest path (in terms of hop count) is always used.

Configuring Global DVMRP Settings

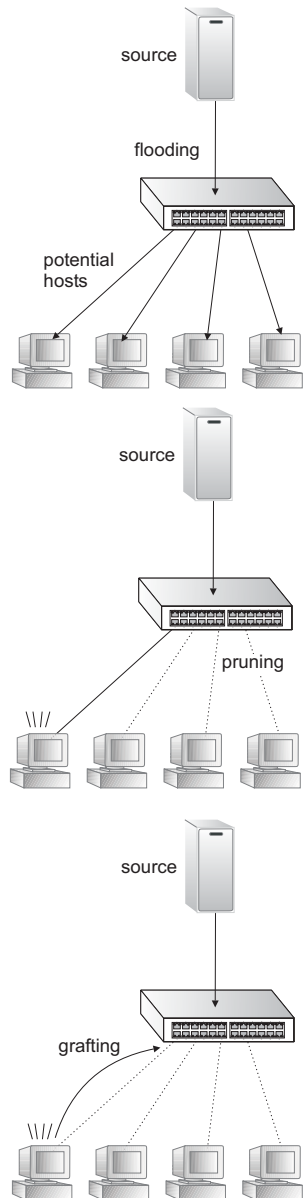
DVMRP is used to route multicast traffic to nodes which have requested a specific multicast service via IGMP. This router uses Reverse Path Forwarding (RPF) to build a shortest-path delivery tree that begins at the source and spreads out to reach group members through the network. RPF uses three different techniques to dynamically reconfigure the multicast spanning tree: broadcasting, pruning, and grafting.

Command Usage

Broadcasting periodically floods the network with traffic from any active multicast server. If IGMP snooping is disabled, multicast traffic is flooded to all ports on the router. However, if IGMP snooping is enabled, then the first packet for any source group pair is flooded to all DVMRP downstream neighbors. If a packet is received through an interface that the router determines to be the shortest path back to the source (based on interface metrics), then the router forwards the packet on all interfaces except for the incoming interface.

The router will transmit a prune message back out the receiving interface (i.e., the parent interface) to its upstream neighboring router if there are no group members on its child interfaces. A prune message tells the upstream router to stop forwarding packets for a particular source-group pair for the prune lifetime.

If the router that previously sent a prune message now discovers a new group member on one of its connections, it sends a graft message to the upstream router. When an upstream router receives this message, it cancels the prune message. If necessary, graft messages are propagated back toward the source until reaching the nearest live branch in the multicast tree.



The global settings that control the prune and graft messages (i.e., prune lifetime) should be configured to the same values on all routers throughout the network to allow DVMRP to function properly. However, if you encounter problems in maintaining a multicast flow, then you may need to modify the protocol variables which control the exchange of topology information between DVMRP routers; such as the probe interval, neighbor timeout or report interval.

Command Attributes

- **DVMRP Protocol** – Enables/disables DVMRP globally. (Default: Disabled)
- **Probe Interval** – Sets the interval for sending neighbor probe messages to the multicast group address for all DVMRP routers. Probe messages are sent to neighboring DVMRP routers from which this device has received probes, and is used to verify whether or not these neighbors are still active members of the multicast tree. (Range: 1-65535 seconds; Default: 10 seconds)
- **Neighbor Timeout Interval** – Sets the interval to wait for messages from a DVMRP neighbor before declaring it dead. This command is used for timing out routes, and for setting the children and leaf flags. (Range: 1-65535 seconds; Default: 35 seconds)
- **Report Interval** – Specifies how often to propagate the complete set of routing tables to other neighbor DVMRP routers. (Range: 1-65535 seconds; Default: 60 seconds)
- **Flash Update Interval** – Specifies how often to send trigger updates, which reflect changes in the network topology.
- **Prune Lifetime** – Specifies how long a prune state will remain in effect for a multicast tree. (Range: 1-65535; Default: 7200 seconds)
- **Default Gateway*** – Specifies the default DVMRP gateway for IP multicast traffic. (Default: none)
 - The specified interface advertises itself as a default route to neighboring DVMRP routers. It advertises the default route out through its other interfaces. Neighboring routers on the other interfaces return Poison Reverse messages for the default route back

to the router. When the router receives these messages, it records all the downstream routers for the default route.

- When multicast traffic with an unknown source address (i.e., not found in the route table) is received on the default upstream route interface, the router forwards this traffic out through the other interfaces (with known downstream routers). However, when multicast traffic with an unknown source address is received on another interface, the router drops it because only the default upstream interface can forward multicast traffic from an unknown source.

* CLI only.

Web – Click Routing Protocol, DVMRP, General Settings. Enable or disable DVMRP. Set the global parameters that control neighbor timeout, the exchange of routing information, or the prune lifetime, and click Apply.

DVMRP General Settings	
DVMRP Protocol	Enabled ▾
Probe Interval (seconds)	10
Neighbor Timeout Interval (seconds)	35
Report Interval (seconds)	60
Flash Update Interval (seconds)	5
Prune Lifetime (seconds)	7200

CLI – This sets the global parameters for DVMRP and displays the current settings.

```

Console(config)#router dvmrp                                4-291
Console(config-router)#probe-interval 30                   4-292
Console(config-router)#nbr-timeout 40                       4-293
Console(config-router)#report-interval 90                   4-293
Console(config-router)#flash-update-interval 10             4-294
Console(config-router)#prune-lifetime 5000                  4-294
Console(config-router)#default-gateway 10.1.0.253           4-295
Console(config-router)#end
Console#show router dvmrp                                    4-298
Admin Status                : enable
Probe Interval               : 10
Nbr expire                   : 35
Minimum Flash Update Interval : 5
prune lifetime               : 7200
route report                  : 60
Default Gateway               :
Console#

```

Configuring DVMRP Interface Settings

To fully enable DVMRP, you need to enable multicast routing globally for the router (page 3-219), enable DVMRP globally for the router (page 3-223), and also enable DVMRP for each interface that will participate in multicast routing.

Command Attributes

DVMRP Interface Information

- **Interface** – VLAN interface on this router that has enabled DVMRP.
- **Address** – IP address of this VLAN interface.
- **Metric** – The metric for this interface used to calculate distance vectors.
- **Status** – Shows that DVMRP is enabled on this interface.

DVMRP Interface Settings

- **VLAN** – Selects a VLAN interface on this router.
- **Metric** – Sets the metric for this interface used to calculate distance vectors.

- **Status** – Enables or disables DVMRP.
 - If DVMRP is enabled on any interface, Layer 3 IGMP should also be enabled on the router (page 3-144).
 - If DVMRP is disabled, the interface cannot propagate IP multicast routing information. However, as long as IGMP snooping is enabled, the interface will still forward multicast traffic to downstream group members within the VLAN. But if IGMP snooping is disabled, then the interface will flood incoming multicast traffic to all ports in the attached VLAN.

Web – Click Routing Protocol, DVMRP, Interface Settings. Select a VLAN from the drop-down box under DVMRP Interface Settings, modify the Metric if required, set the Status to Enabled or Disabled, and click Apply.

DVMRP Interface Information

Interface	Address	Metric	Status
VLAN1	10.1.0.253	1	Enabled
VLAN2	10.1.1.253	1	Enabled

Entry Count: 2

DVMRP Interface Settings

VLAN	4
Metric (1 - 31)	
Status	Disabled

CLI – This example enables DVMRP and sets the metric for VLAN 1.

```

Console(config)#interface vlan 1                                4-119
Console(config-if)#ip dvmrp                                     4-296
Console(config-if)#ip dvmrp metric 2                           4-297
Console(config-if)#end
Console#show ip dvmrp interface                                4-301
Vlan 1 is up
  DVMRP is enabled
  Metric is 2
Console#
    
```

Displaying Neighbor Information

You can display all the neighboring DVMRP routers.

Command Attributes

- **Neighbor Address** – The IP address of the network device immediately upstream for this multicast delivery tree.
- **Interface** – The IP interface on this router that connects to the upstream neighbor.
- **Up time** – The time since this device last became a DVMRP neighbor to this router.
- **Expire** – The time remaining before this entry will be aged out.
- **Capabilities** – A hexadecimal value that indicates the neighbor's capabilities. Each time a probe message is received from a neighbor, the router compares the capabilities bits with the previous version for that neighbor to check for changes in neighbor capabilities. (Refer to DVMRP IETF Draft v3-10 section 3.2.1 for a detailed description of these bits). These bits are described below:
 - Leaf (bit 0) - Neighbor has only one interface with neighbors.
 - Prune (bit 1) - Neighbor supports pruning.
 - Generation ID (bit 2) - Neighbor sends its Generation ID in probe messages.
 - Mtrace (bit 3) - Neighbor can handle multicast trace requests.
 - SNMP (bit 4) - Neighbor is SNMP capable.
 - Netmask - (bit 5) - Neighbor will accept network masks appended to the prune, graft, and graft acknowledgement messages.
 - Reserved (bit 6 and 7) - Reserved for future use.

Web – Click Routing Protocol, DVMRP, Neighbor Information.

DVMRP Neighbor Information

Neighbor Address	Interface	Up time	Expire	Capabilities
10.1.0.254	VLAN1	79215	31	6

Entry Count: 1

CLI – This example displays the only neighboring DVMRP router.

Console#show ip dvmrp neighbor					4-300
Address	Interface	Uptime	Expire	Capabilities	

10.1.0.254	vlan1	79315	32	6	
Console#					

Displaying the Routing Table

The router learns source-routed information from neighboring DVMRP routers and also advertises learned routes to its neighbors. The router merely records path information it has learned on its own or from other routers. It does not consider group membership or prune messages. Information stored in the routing table includes subnetworks from which IP multicast traffic originates, upstream routers that have sent multicast traffic in the past or have been learned through routing messages exchanged with other routers, interfaces connected to an upstream router, or outgoing interfaces that are connected to multicast hosts.

The DVMRP routing table contains multicast route information learned via DVMRP route updates, and is used to forward IP multicast traffic. The routes listed in the table do not reflect actual multicast traffic flows. For this information, you should look at the IGMP Member Port Table (page 3-143) or the IGMP Group Membership Table (page 3-148).

Command Attributes

- **IP Address** – IP subnetwork that contains a multicast source, an upstream router, or an outgoing interface connected to multicast hosts.
- **Netmask** – Subnet mask that is used for the source address. This mask identifies the host address bits used for routing to specific subnets.
- **Upstream Neighbor** – IP address of the network device immediately upstream for each multicast group.
- **Interface** – The IP interface on this router that connects to the upstream neighbor.
- **Metric** – The metric for this interface used to calculate distance vectors.

- **Up time** – The time elapsed since this entry was created.
- **Expire** – The time remaining before this entry will be aged out.

Web – Click Routing Protocol, DVMRP, DVMRP Routing Table.

Ip Address	Netmask	Upstream Neighbor	Interface	Metric	Up time	Expire
10.1.0.0	255.255.255.0	10.1.0.253	VLAN1	1	84279	0
10.1.1.0	255.255.255.0	10.1.1.253	VLAN2	1	84828	0
10.1.8.0	255.255.255.0	10.1.0.254	VLAN1	2	19570	134

Entry Count: 3

CLI – This example displays known DVMRP routes.

Console#show ip dvmrp route						4-299	
Source	Mask	Upstream_nbr	Interface	Metric	UpTime	Expire	
10.1.0.0	255.255.255.0	10.1.0.253	vlan1	1	84438	0	
10.1.1.0	255.255.255.0	10.1.1.253	vlan2	1	84987	0	
10.1.8.0	255.255.255.0	10.1.0.254	vlan1	2	19729	97	
Console#							

Configuring PIM-DM

Protocol-Independent Multicasting (PIM) provides two different modes of operation: sparse mode and dense mode. Sparse mode (SM) is designed for networks where the probability of multicast group members is low, such as the Internet. Dense mode (DM), on the other hand, is designed for networks where the probability of multicast group members is high, such as a local network.

PIM-DM is a simple multicast routing protocol that uses flood and prune to build a source-routed multicast delivery tree for each multicast source-group pair. It is simpler than DVMRP because it does not maintain its own routing table. Instead, it uses the routing table provided by the unicast routing protocol enabled on the router interface. When the router receives a multicast packet for a source-group pair, PIM-DM checks the unicast routing table on the inbound interface to determine if this is the same interface used for routing unicast packets to the multicast source

network. If it is not, the router drops the packet and sends a prune message back out the source interface. If it is the same interface used by the unicast protocol, then the router forwards a copy of the packet to all the other interfaces for which it has not already received a prune message for this specific source-group pair.

DVMRP holds the prune state for about two hours, while PIM-DM holds it for only about three minutes. This results in more flooding than encountered with DVMRP, but this is the only major trade-off for the lower processing overhead and simplicity of configuration for PIM-DM.

Configuring Global PIM-DM Settings

PIM-DM is used to route multicast traffic to nodes which have requested a specific multicast service via IGMP. It uses the router's unicast routing table to determine if the interface through which a packet is received provides the shortest path back to the source. This is done on a per hop basis back toward the source of the multicast delivery tree. PIM-DM uses three different techniques to dynamically reconfigure the multicast spanning tree: broadcasting, pruning, and grafting.

To use PIM-DM, you must enable it globally for the router as described below, and for each interface that will support multicast routing as described in the next section. Also note that IGMP must be enabled to allow the router to determine the location of group members.

Web – Click Routing Protocol, PIM-DM, General Settings. Enable or disable PIM-DM globally for the router, and click Apply.

PIM-DM General Settings

PIM-DM Protocol

CLI – This example enables PIM-DM globally and displays the current status.

Console(config)#router pim	4-302
Console#show router pim	4-308
Admin Status: Enabled	
Console#	

Configuring PIM-DM Interface Settings

To fully enable PIM-DM, you need to enable multicast routing globally for the router (page 3-219), enable PIM-DM globally for the router (page 3-232), and also enable PIM-DM for each interface that will participate in multicast routing.

Command Usage

- PIM-DM functions similar to DVMRP by periodically flooding the network with traffic from any active multicast server (page 3-222). It also uses IGMP to determine the presence of multicast group members. The main difference, is that it uses the router's unicast routing table to determine if the interface through which a packet is received provides the shortest path back to the source.
- Dense-mode interfaces are subject to multicast flooding by default, and are only removed from the multicast routing table when the router determines that there are no group members or downstream routers, or when a prune message is received from a downstream router.
- The interface settings that control the prune and graft messages (i.e., prune holdtime) should be configured to the same values on all routers throughout the network to allow PIM to function properly.

Command Attributes

- **VLAN** – Selects a VLAN interface on this router.
- **PIM-DM Protocol Status** – Enables/disables PIM-DM. (Default: Disabled)
- **Hello Interval** – Sets the frequency at which PIM hello messages are transmitted. Hello messages are sent to neighboring PIM routers from which this device has received probes, and are used to verify whether or

not these neighbors are still active members of the multicast tree. (Range: 1-65535 seconds; Default: 30)

- **Hello Holdtime** – Sets the interval to wait for hello messages from a neighboring PIM router before declaring it dead. Note that the hello holdtime should be 3.5 times the value of Hello Interval. (Range: 1-65535 seconds; Default: 105)
- **Trigger Hello Interval** – Configures the maximum time before transmitting a triggered PIM hello message after the router is rebooted or PIM is enabled on an interface. (Range: 1-65535 seconds; Default: 5)
 - When a router first starts or PIM is enabled on an interface, the hello-interval is set to random value between 0 and the Trigger Hello Interval. This prevents synchronization of Hello messages on multi-access links if multiple routers are powered on simultaneously.
 - Also, if a Hello message is received from a new neighbor, the receiving router will send its own Hello message after a random delay between 0 and the Trigger Hello Interval.
- **Prune Holdtime** – Configures of the hold time for the prune state. The multicast interface that first receives a multicast stream from a particular source forwards this traffic to all other PIM interfaces on the router. If there are no requesting groups on that interface, the leaf node sends a prune message upstream and enters a prune state for this multicast stream. The prune state is maintained until the prune holdtime timer expires or a graft message is received for the forwarding entry. (Range: 1-65535 seconds; Default: 210)
- **Graft Retry Interval** – Configures the time to wait for a graft acknowledgement before resending a graft. A graft message is sent by a router to cancel a prune state. When a router receives a graft message, it must respond with an graft acknowledgement message. If this acknowledgement message is lost, the router that sent the graft message will resend it a maximum number of times as defined by Max Graft Retries. (Range: 1-65535 seconds; Default: 3)
- **Max Graft Retries** – Configures the maximum number of times to resend a graft message if it has not been acknowledged. (Range: 1-65535; Default: 2)

Web – Click Routing Protocol, PIM-DM, Interface Settings. Select a VLAN, enable or disable PIM-DM for the selected interface, modify any of the protocol parameters as required, and click Apply.

PIM-DM Interface Settings	
VLAN	<input type="text" value="2"/>
PIM-DM Protocol Status	<input type="text" value="Enabled"/>
Hello Interval (seconds)	<input type="text" value="30"/>
Hello Holdtime (seconds)	<input type="text" value="105"/>
Trigger Hello Interval (seconds)	<input type="text" value="5"/>
Join/Prune Holdtime (seconds)	<input type="text" value="210"/>
Graft Retry Interval (seconds)	<input type="text" value="3"/>
Max Graft Retries	<input type="text" value="2"/>

CLI – This example sets the PIM-DM protocol parameters for VLAN 2, and displays the current settings.

```

Console(config)#interface vlan 2                                4-165
Console(config-if)#ip pim dense-mode                            4-303
Console(config-if)#ip pim hello-interval 60                    4-304
Console(config-if)#ip pim hello-holdtime 210                   4-305
Console(config-if)#ip pim trigger-hello-interval 10            4-305
Console(config-if)#ip pim join-prune-holdtime 60                4-306
Console(config-if)#ip pim graft-retry-interval 9                4-307
Console(config-if)#ip pim max-graft-retries 5                  4-308
Console(config-if)#end
Console#show ip pim interface 2                                  4-309
Vlan 2 is up
PIM is enabled, mode is Dense.
Internet address is 10.1.1.253.
Hello time interval is 60 sec, trigger hello time interval is 10 sec.
Hello holdtime is 210 sec.
Join/Prune holdtime is 60 sec.
Graft retry interval is 9 sec, max graft retries is 5.
DR Internet address is 10.1.1.253, neighbor count is 0.

Console#

```

Displaying Interface Information

You can display a summary of the current interface status for PIM-DM, including the number of neighboring PIM routers, and the address of the designated PIM router.

Command Attributes

- **Interface** – A VLAN interface on this router.
- **Address** – The IP address for this interface.
- **Mode** – The PIM mode in use. (This router only supports Dense Mode at this time.)
- **Neighbor Count** – The number of PIM neighbors detected on this interface.
- **DR Address** – The designated PIM router for this interface.

Web – Click Routing Protocol, PIM-DM, Interface Information.

PIM-DM Interface Information

Interface	Address	Mode	Neighbor Count	DR Address
VLAN1	10.1.0.252	Dense	1	10.1.0.253
VLAN10	10.1.9.252	Dense	0	10.1.9.252

Entry Count: 2

CLI – This example shows the PIM-DM interface summary for VLAN 1.

```

Console#show ip pim interface 1                                     4-309
Vlan 1 is up
PIM is enabled, mode is Dense.
Internet address is 10.1.0.253.
Hello time interval is 30 sec, trigger hello time interval is 5 sec.
Hello holdtime is 105 sec.
Join/Prune holdtime is 210 sec.
Graft retry interval is 3 sec, max graft retries is 2.
DR Internet address is 10.1.0.253, neighbor count is 1.

Console#

```

Displaying Neighbor Information

You can display all the neighboring PIM-DM routers.

Command Attributes

- **Neighbor Address** – IP address of the next-hop router.
- **Interface** – VLAN that is attached to this neighbor.
- **Up time** – The duration this entry has been active.
- **Expire** – The time before this entry will be removed.
- **Mode** – PIM mode used on this interface. (Only Dense Mode is supported.)

Web – Click Routing Protocol, PIM-DM, Neighbor Information.

PIM-DM Neighbor Information				
Neighbor Address	Interface	Up time	Expire	Mode
10.1.0.253	VLAN1	596	78	
Entry Count: 1				

CLI – This example displays the only neighboring PIM-DM router.

Console#show ip pim neighbor						4-309
Address	VLAN	Interface	Uptime	Expire	Mode	
-----	-----	-----	-----	-----	-----	
10.1.0.253		1	613	91	Dense	
Console#						

CHAPTER 4

COMMAND LINE INTERFACE

This chapter describes how to use the Command Line Interface (CLI).

Using the Command Line Interface

Accessing the CLI

When accessing the management interface for the switch over a direct connection to the server's console port, or via a Telnet connection, the switch can be managed by entering command keywords and parameters at the prompt. Using the switch's command-line interface (CLI) is very similar to entering commands on a UNIX system.

Console Connection

To access the switch through the console port, perform these steps:

1. At the console prompt, enter the user name and password. (The default user names are “admin” and “guest” with corresponding passwords of “admin” and “guest.”) When the administrator user name and password is entered, the CLI displays the “Console#” prompt and enters privileged access mode (i.e., Privileged Exec). But when the guest user name and password is entered, the CLI displays the “Console>” prompt and enters normal access mode (i.e., Normal Exec).
2. Enter the necessary commands to complete your desired tasks.

3. When finished, exit the session with the “quit” or “exit” command.

After connecting to the system through the console port, the login screen displays:

```
User Access Verification

Username: admin
Password:

      CLI session with the SMC6724L3 1 Intelligent Switch is opened.
      To end the CLI session, enter [Exit].

Console#
```

Telnet Connection

Telnet operates over the IP transport protocol. In this environment, your management station and any network device you want to manage over the network must have a valid IP address. Valid IP addresses consist of four numbers, 0 to 255, separated by periods. Each address consists of a network portion and host portion. For example, the IP address assigned to this switch, 10.1.0.1, consists of a network portion (10.1.0) and a host portion (1).

Note: The IP address for this switch is unassigned by default.

To access the switch through a Telnet session, you must first set the IP address for the switch, and set the default gateway if you are managing the switch from a different IP subnet. For example,

```
Console(config)#interface vlan 1
Console(config-if)#ip address 10.1.0.254 255.255.255.0
Console(config-if)#exit
Console(config)#ip default-gateway 10.1.0.254
```

If your corporate network is connected to another network outside your office or to the Internet, you need to apply for a registered IP address. However, if you are attached to an isolated network, then you can use any IP address that matches the network segment to which you are attached.

After you configure the switch with an IP address, you can open a Telnet session by performing these steps:

1. From the remote host, enter the Telnet command and the IP address of the device you want to access.
2. At the prompt, enter the user name and system password. The CLI will display the “Vty-0#” prompt for the administrator to show that you are using privileged access mode (i.e., Privileged Exec), or “Vty-0>” for the guest to show that you are using normal access mode (i.e., Normal Exec).
3. Enter the necessary commands to complete your desired tasks.
4. When finished, exit the session with the “quit” or “exit” command.

After entering the Telnet command, the login screen displays:

```
Username: admin
Password:

      CLI session with the SMC6724L3 1 Switch is opened.
      To end the CLI session, enter [Exit].

Vty-0#
```

Note: You can open up to four sessions to the device via Telnet.

Entering Commands

This section describes how to enter CLI commands.

Keywords and Arguments

A CLI command is a series of keywords and arguments. Keywords identify a command, and arguments specify configuration parameters. For example, in the command “show interfaces status ethernet 1/5,” **show** **interfaces** and **status** are keywords, **ethernet** is an argument that specifies the interface type, and **1/5** specifies the unit/port.

You can enter commands as follows:

- To enter a simple command, enter the command keyword.
- To enter multiple commands, enter each command in the required order. For example, to enable Privileged Exec command mode, and display the startup configuration, enter:

```
Console>enable  
Console#show startup-config
```

- To enter commands that require parameters, enter the required parameters after the command keyword. For example, to set a password for the administrator, enter:

```
Console(config)#username admin password 0 smith
```

Minimum Abbreviation

The CLI will accept a minimum number of characters that uniquely identify a command. For example, the command “configure” can be entered as **con**. If an entry is ambiguous, the system will prompt for further input.

Command Completion

If you terminate input with a Tab key, the CLI will print the remaining characters of a partial keyword up to the point of ambiguity. In the “logging history” example, typing **log** followed by a tab will result in printing the command up to “**logging**.”

Getting Help on Commands

You can display a brief description of the help system by entering the **help** command. You can also display command syntax by using the “?” character to list keywords or parameters.

Showing Commands

If you enter a “?” at the command prompt, the system will display the first level of keywords for the current command class (Normal Exec or Privileged Exec) or configuration class (Global, ACL, DHCP, Interface, Line, Router or VLAN Database). You can also display a list of valid keywords for a specific command. For example, the command “**show ?**” displays a list of possible show commands:

```

Console#show ?
  access-group      Access groups
  access-list       Access lists
  arp               Information of arp cache
  bridge-ext        Bridge extend information
  dot1x             Show 802.1x content
  garp              Garp property
  gvrp              Show GVRP information of interface
  history           Information of history
  interfaces         Information of interfaces
  ip                IP information
  line              TTY line information
  logging           Show the contents of logging buffers
  mac               MAC access lists
  mac-address-table Set configuration of the address table
  map               Map priority
  port              Characteristics of the port
  pvlan             Information of private VLAN
  queue             Information of priority queue
  radius-server     RADIUS server information
  rip               Rip
  router            Router
  running-config    The system configuration of running
  snmp              SNMP statistics
  sntp              Sntp
  spanning-tree     Specify spanning-tree
  startup-config    The system configuration of starting up
  system            Information of system
  users             Display information about terminal lines
  version           System hardware and software status
  vlan              Switch VLAN Virtual Interface
Console#show

```

The command “**show interfaces ?**” will display the following information:

```

Console>show interfaces ?
  counters      Information of interfaces counters
  status        Information of interfaces status
  switchport    Information of interfaces switchport

```

Partial Keyword Lookup

If you terminate a partial keyword with a question mark, alternatives that match the initial letters are provided. (Remember not to leave a space between the command and question mark.) For example “**s?**” shows all the keywords starting with “s.”

```
Console#show s?  
snmp          startup-config  system
```

Negating the Effect of Commands

For many configuration commands you can enter the prefix keyword “**no**” to cancel the effect of a command or reset the configuration to the default value. For example, the **logging** command will log system messages to a host server. To disable logging, specify the **no logging** command. This guide describes the negation effect for all applicable commands.

Using Command History

The CLI maintains a history of commands that have been entered. You can scroll back through the history of commands by pressing the up arrow key. Any command displayed in the history list can be executed again, or first modified and then executed.

Using the **show history** command displays a longer list of recently executed commands.

Understanding Command Modes

The command set is divided into Exec and Configuration classes. Exec commands generally display information on system status or clear statistical counters. Configuration commands, on the other hand, modify interface parameters or enable certain switching functions. These classes are further divided into different modes. Available commands depend on the selected mode. You can always enter a question mark “**?**” at the prompt to display a list of the commands available for the current mode. The

command classes and associated modes are displayed in the following table:

Class	Mode	
Exec	Normal Privileged	
Configuration	Global*	Access Control List DHCP Interface Line Router VLAN Database

* You must be in Privileged Exec mode to access the Global configuration mode.

You must be in Global Configuration mode to access any of the other configuration modes.

Exec Commands

When you open a new console session on the switch with the user name and password “guest,” the system enters the Normal Exec command mode (or guest mode), displaying the “Console>” command prompt. Only a limited number of the commands are available in this mode. You can access all commands only from the Privileged Exec command mode (or administrator mode). To access Privilege Exec mode, open a new console session with the user name and password “admin.” The system will now display the “Console#” command prompt. You can also enter Privileged Exec mode from within Normal Exec mode, by entering the **enable** command, followed by the privileged level password “super” (page 4-34).

To enter Privileged Exec mode, enter the following user names and passwords:

```

Username: admin
Password: [admin login password]

      CLI session with the SMC6724L3 1 Switch is opened.
      To end the CLI session, enter [Exit].

Console#

```

```
Username: guest
Password: [guest login password]

      CLI session with the SMC6724L3 1 Switch is opened.
      To end the CLI session, enter [Exit].

Console#enable
Password: [privileged level password]
Console#
```

Configuration Commands

Configuration commands are privileged level commands used to modify switch settings. These commands modify the running configuration only and are not saved when the switch is rebooted. To store the running configuration in non-volatile storage, use the **copy running-config startup-config** command.

The configuration commands are organized into different modes:

- Global Configuration - These commands modify the system level configuration, and include commands such as **hostname** and **snmp-server community**.
- Access Control List Configuration - These commands are used for packet filtering.
- DHCP Configuration - These commands are used to configure the DHCP server.
- Interface Configuration - These commands modify the port configuration such as **speed-duplex** and **negotiation**.
- Line Configuration - These commands modify the console port and Telnet configuration, and include command such as **parity** and **databits**.
- Router Configuration - These commands configure global settings for unicast and multicast routing protocols.
- VLAN Configuration - Includes the command to create VLAN groups.

To enter the Global Configuration mode, enter the command **configure** in Privileged Exec mode. The system prompt will change to “Console(config)#” which gives you access privilege to all Global Configuration commands.

```
Console#configure
Console(config)#
```

To enter the other modes, at the configuration prompt type one of the following commands. Use the **exit** or **end** command to return to the Privileged Exec mode.

Mode	Command	Prompt	Page
Line	line {console vty}	Console(config-line)#	4-13
Access Control List	access-list ip standard access-list ip extended access-list mac	Console(config-std-acl) Console(config-ext-acl) Console(config-mac-acl)	4-74
DHCP	ip dhcp pool	Console(config-dhcp)	4-97
Interface	interface {ethernet <i>port</i> port-channel <i>id</i> vlan <i>id</i> }	Console(config-if)#	4-118
VLAN	vlan database	Console(config-vlan)	4-162
Router	router {rip ospf dvmrp pim}	Console(config-router)	4-231 4-246 4-291 4-302

For example, you can use the following commands to enter interface configuration mode, and then return to Privileged Exec mode

```
Console(config)#interface ethernet 1/5
.
.
.
Console(config-if)#exit
Console(config)#
```

Command Line Processing

Commands are not case sensitive. You can abbreviate commands and parameters as long as they contain enough letters to differentiate them from any other currently available commands or parameters. You can use the Tab key to complete partial commands, or enter a partial command followed by the “?” character to display a list of possible matches. You can also use the following editing keystrokes for command-line processing:

Keystroke	Function
Ctrl-A	Shifts cursor to start of command line.
Ctrl-B	Shifts cursor to the left one character.
Ctrl-C	Terminates the current task and displays the command prompt.
Ctrl-E	Shifts cursor to end of command line.
Ctrl-F	Shifts cursor to the right one character.
Ctrl-K	Deletes all characters from the cursor to the end of the line.
Ctrl-L	Repeats current command line on a new line.
Ctrl-P	Shows the last command.
Ctrl-R	Repeats current command line on a new line.
Ctrl-U	Deletes the entire line.
Ctrl-W	Deletes the last word typed.
Esc-B	Moves the cursor back one word.
Esc-D	Deletes from the cursor to the end of the word.
Esc-F	Moves the cursor forward one word.
Delete key or backspace key	Erases a mistake when entering a command.

Command Groups

The system commands can be broken down into the functional groups shown below.

Command Group	Description	Page
Line	Sets communication parameters for the serial port and Telnet, including baud rate and console time-out	4-13
General	Basic commands for entering privileged access mode, restarting the system, or quitting the CLI	4-24
System Management	Controls system logs, system passwords, user name, browser management options, and a variety of other system information	4-31
Flash/File	Manages code image or switch configuration files	4-53
Authentication	Configures logon access using local or RADIUS authentication; also configures IEEE 802.1x port access control	4-60
Access Control List	Provides filtering for IP frames (based on address, protocol, TCP/UDP port number or TCP control code) or non-IP frames (based on MAC address or Ethernet type)	4-74
SNMP	Activates authentication failure traps; configures community access strings, and trap managers	4-90
DHCP	Configures DHCP client, relay and server functions	4-97
Interface	Configures the connection parameters for all Ethernet ports, aggregated links, and VLANs	4-118
Mirror Port	Mirrors data to another port for analysis without affecting the data passing through or the performance of the monitored port	4-133
Rate Limiting	Controls the maximum rate for traffic transmitted or received on a port	4-135
Link Aggregation	Statically groups multiple ports into a single logical trunk; configures Link Aggregation Control Protocol for port trunks	4-137
Address Table	Configures the address table for filtering specified addresses, displays current entries, clears the table, or sets the aging time	4-141

Command Group	Description	Page
Spanning Tree	Configures Spanning Tree settings for the switch	4-146
VLANs	Configures VLAN settings, and defines port membership for VLAN groups; also enables or configures private VLANs	4-162
GVRP and Bridge Extension	Configures GVRP settings that permit automatic VLAN learning; shows the configuration for the bridge extension MIB	4-175
Priority	Sets port priority for untagged frames, relative weight for each priority queue, also sets priority for TCP traffic types, IP precedence, and DSCP	4-181
Multicast Filtering	Configures IGMP multicast filtering, query parameters, and specifies ports attached to a multicast router	4-196
IP Interface	Configures IP address for the switch interfaces; also configures ARP parameters and static entries	4-215
IP Routing	Configures static and dynamic unicast routing	4-225
Multicast Routing	Configures multicast routing protocols DVMRP and PIM-DM	4-285

The access mode shown in the following tables is indicated by these abbreviations:

NE (Normal Exec)	IC (Interface Configuration)
PE (Privileged Exec)	LC (Line Configuration)
GC (Global Configuration)	RC (Router Configuration)
ACL (Access Control List Config.)	VC (VLAN Database Configuration)
DC (DHCP Server Configuration)	

Line Commands

You can access the onboard configuration program by attaching a VT100 compatible device to the server's serial port. These commands are used to set communication parameters for the serial port or Telnet (i.e., a virtual terminal).

Command	Function	Mode	Page
line	Identifies a specific line for configuration and starts the line configuration mode	GC	4-14
login	Enables password checking at login	LC	4-15
password	Specifies a password on a line	LC	4-16
exec-timeout	Sets the interval that the command interpreter waits until user input is detected	LC	4-17
password-thresh	Sets the password intrusion threshold, which limits the number of failed logon attempts	LC	4-18
silent-time*	Sets the amount of time the management console is inaccessible after the number of unsuccessful logon attempts exceeds the threshold set by the password-thresh command	LC	4-19
databits*	Sets the number of data bits per character that are interpreted and generated by hardware	LC	4-20
parity*	Defines the generation of a parity bit	LC	4-21
speed*	Sets the terminal baud rate	LC	4-22
stopbits*	Sets the number of the stop bits transmitted per byte	LC	4-23
show line	Displays a terminal line's parameters	NE, PE	4-23

* These commands only apply to the serial port.

line

Use this command to identify a specific line for configuration, and to process subsequent line configuration commands.

Syntax

line {**console** | **vty**}

- **console** - Console terminal line.
- **vty** - Virtual terminal for remote console access (i.e., Telnet).

Default Setting

There is no default line.

Command Mode

Global Configuration

Command Usage

Telnet is considered a virtual terminal connection and will be shown as “Vty” in screen displays such as `show users`. However, the serial communication parameters (e.g., databits) do not affect Telnet connections.

Example

To enter console line mode, enter the following command:

```
Console(config)#line console
Console(config-line)#
```

Related Commands

`show line` (4-23)
`show users` (4-51)

login

Use this command to enable password checking at login. Use the **no** form to disable password checking and allow connections without a password.

Syntax

login [**local**]

no login

local - Selects local password checking. Authentication is based on the user name specified with the **username** command.

Default Setting

login local

Command Mode

Line Configuration

Command Usage

- There are three authentication modes provided by the switch at login:
 - **login** selects authentication by a single global password as specified by the **password** line configuration command. When using this method, the management interface starts in Normal Exec (NE) mode.
 - **login local** selects authentication via the user name and password specified by the **username** command (i.e., default setting). When using this method, the management interface starts in Normal Exec (NE) or Privileged Exec (PE) mode, depending on the user's privilege level (0 or 15 respectively).
 - **no login** selects no authentication. When using this method, the management interface starts in Normal Exec (NE) mode.
- This command controls login authentication via the switch itself. To configure user names and passwords for remote authentication servers, you must use the RADIUS software installed on those servers.

Example

```
Console(config-line)#login local
Console(config-line)#
```

Related Commands

username (4-33)

password (4-16)

password

Use this command to specify the password for a line. Use the **no** form to remove the password.

Syntax

password {0 | 7} *password*

no password

- {0 | 7} - 0 means plain password, 7 means encrypted password
- *password* - Character string that specifies the line password.
(Maximum length: 8 characters plain text, 32 encrypted, case sensitive)

Default Setting

No password is specified.

Command Mode

Line Configuration

Command Usage

- When a connection is started on a line with password protection, the system prompts for the password. If you enter the correct password, the system shows a prompt. You can use the **password-thresh** command to set the number of times a user can enter an incorrect password before the system terminates the line connection and returns the terminal to the idle state.
- The encrypted password is required for compatibility with legacy password settings (i.e., plain text or encrypted) when reading the

configuration file during system bootup or when downloading the configuration file from a TFTP server. There is no need for you to manually configure encrypted passwords.

Example

```
Console(config-line)#password 0 secret
Console(config-line)#
```

Related Commands

login (4-15)
password-thresh (4-18)

exec-timeout

Use this command to set the interval that the system waits until user input is detected. Use the **no** form to restore the default.

Syntax

exec-timeout [*seconds*]
no exec-timeout
seconds - Integer that specifies the number of seconds.
(Range: 0 - 65535 seconds; 0: no timeout)

Default Setting

CLI: No timeout
Telnet: 10 minutes

Command Mode

Line Configuration

Command Usage

- If user input is detected within the timeout interval, the session is kept open; otherwise the session is terminated.
- This command applies to both the local console and Telnet connections.
- The timeout for Telnet cannot be disabled.

Example

To set the timeout to two minutes, enter this command:

```
Console(config-line)#exec-timeout 120
Console(config-line)#
```

password-thresh

Use this command to set the password intrusion threshold which limits the number of failed logon attempts. Use the **no** form to remove the threshold value.

Syntax

password-thresh [*threshold*]

no password-thresh

threshold - The number of allowed password attempts.

(Range: 1-120; 0: no threshold)

Default Setting

The default value is three attempts.

Command Mode

Line Configuration

Command Usage

- When the logon attempt threshold is reached, the system interface becomes silent for a specified amount of time before allowing the next logon attempt. (Use the **silent-time** command to set this interval.) When this threshold is reached for Telnet, the Telnet logon interface shuts down.
- This command applies to both the local console and Telnet connections.

Example

To set the password threshold to five attempts, enter this command:

```
Console(config-line)#password-thresh 5
Console(config-line)#
```


Related Commands

silent-time (4-19)

silent-time

Use this command to set the amount of time the management console is inaccessible after the number of unsuccessful logon attempts exceeds the threshold set by the **password-thresh** command. Use the **no** form to remove the silent time value.

Syntax

silent-time [*seconds*]

no silent-time

seconds - The number of seconds to disable console response.
(Range: 0-65535; 0: no silent-time)

Default Setting

The default value is no silent-time.

Command Mode

Line Configuration

Example

To set the silent time to 60 seconds, enter this command:

```
Console(config-line)#silent-time 60
Console(config-line)#
```

Related Commands

password-thresh (4-18)

databits

Use this command to set the number of data bits per character that are interpreted and generated by the console port. Use the **no** form to restore the default value.

Syntax

databits {7 | 8}

no databits

- 7 - Seven data bits per character.
- 8 - Eight data bits per character.

Default Setting

8 data bits per character

Command Mode

Line Configuration

Command Usage

The databits command can be used to mask the high bit on input from devices that generate 7 data bits with parity. If parity is being generated, specify 7 data bits per character. If no parity is required, specify 8 data bits per character.

Example

To specify 7 data bits, enter this command:

```
Console(config-line)#databits 7
Console(config-line)#
```

Related Commands

parity (4-21)

parity

Use this command to define generation of a parity bit. Use the **no** form to restore the default setting.

Syntax

parity {**none** | **even** | **odd**}

no parity

- **none** - No parity
- **even** - Even parity
- **odd** - Odd parity

Default Setting

No parity

Command Mode

Line Configuration

Command Usage

Communication protocols provided by devices such as terminals and modems often require a specific parity bit setting.

Example

To specify no parity, enter this command:

```
Console(config-line)#parity none
Console(config-line)#
```

speed

Use this command to set the terminal line's baud rate. This command sets both the transmit (to terminal) and receive (from terminal) speeds. Use the **no** form to restore the default setting.

Syntax

speed *bps*

no speed

bps - Baud rate in bits per second.

(Options: 9600, 19200, 38400, 57600, 115200 bps)

Default Setting

9600 bps

Command Mode

Line Configuration

Command Usage

Set the speed to match the baud rate of the device connected to the serial port. Some baud rates available on devices connected to the port might not be supported. The system indicates if the speed you selected is not supported.

Example

To specify 57600 bps, enter this command:

```
Console(config-line)#speed 57600
Console(config-line)#
```

stopbits

Use this command to set the number of the stop bits transmitted per byte.

Use the **no** form to restore the default setting.

Syntax

stopbits {1 | 2}

- **1** - One stop bit
- **2** - Two stop bits

Default Setting

1 stop bit

Command Mode

Line Configuration

Example

To specify 2 stop bits, enter this command:

```
Console(config-line)#stopbits 2
Console(config-line)#
```

show line

Use this command to display the terminal line's parameters.

Syntax

show line [console | vty]

- **console** - Console terminal line.
- **vtty** - Virtual terminal for remote console access (i.e., Telnet).

Default Setting

Shows all lines

Command Mode

Normal Exec, Privileged Exec

Example

To show all lines, enter this command:

```
Console#show line
Console configuration:
  Password threshold: 3 times
  Interactive timeout: Disabled
  Silent time: Disabled
  Baudrate: 9600
  Databits: 8
  Parity: none
  Stopbits: 1
Vty configuration:
  Password threshold: 3 times
  Interactive timeout: 65535
```

General Commands

Command	Function	Mode	Page
enable	Activates privileged mode	NE	4-25
disable	Returns to normal mode from privileged mode	PE	4-26
configure	Activates global configuration mode	PE	4-27
show history	Shows the command history buffer	NE, PE	4-27
reload	Restarts the system	PE	4-28
end	Returns to Privileged Exec mode	any config. mode	4-29
exit	Returns to the previous configuration mode, or exits the CLI	any	4-29
quit	Exits a CLI session	NE, PE	4-30
help	Shows how to use help	any	NA
?	Shows options for command completion (context sensitive)	any	NA

enable

Use this command to activate Privileged Exec mode. In privileged mode, additional commands are available, and certain commands display additional information. See “Understanding Command Modes” on page 4-6.

Syntax

enable [*level*]

level - Privilege level to log into the device.

The device has two predefined privilege levels: 0: Normal Exec, 15: Privileged Exec. Enter level 15 to access Privileged Exec mode.

Default Setting

Level 15

Command Mode

Normal Exec

Command Usage

- “super” is the default password required to change the command mode from Normal Exec to Privileged Exec. (To set this password, see the **enable password** command on page 4-34.)
- The “#” character is appended to the end of the prompt to indicate that the system is in privileged access mode.

Example

```
Console>enable
Password: [privileged level password]
Console#
```

Related Commands

disable (4-26)

enable password (4-34)

disable

Use this command to return to Normal Exec mode from privileged mode. In normal access mode, you can only display basic information on the switch's configuration or Ethernet statistics. To gain access to all commands, you must use the privileged mode. See “Understanding Command Modes” on page 4-6.

Default Setting

None

Command Mode

Privileged Exec

Command Usage

The “>” character is appended to the end of the prompt to indicate that the system is in normal access mode.

Example

```
Console#disable  
Console>
```

Related Commands

enable (4-25)

configure

Use this command to activate Global Configuration mode. You must enter this mode to modify any settings on the switch. You must also enter Global Configuration mode prior to enabling some of the other configuration modes, including Interface Configuration, Line Configuration, and VLAN Database Configuration. See “Understanding Command Modes” on page 4-6.

Default Setting

None

Command Mode

Privileged Exec

Example

```
Console#configure
Console(config)#
```

Related Commands

end (4-29)

show history

Use this command to show the contents of the command history buffer.

Default Setting

None

Command Mode

Normal Exec, Privileged Exec

Command Usage

The history buffer size is fixed at 10 Execution commands and 10 Configuration commands.

Example

In this example, the show history command lists the contents of the command history buffer:

```
Console#show history
Execution command history:
 2 config
 1 show history

Configuration command history:
 4 interface vlan 1
 3 exit
 2 interface vlan 1
 1 end

Console#
```

The **!** command repeats commands from the Execution command history buffer when you are in Normal Exec or Privileged Exec Mode, and commands from the Configuration command history buffer when you are in any of the configuration modes. In this example, the **!2** command repeats the second command in the Execution history buffer (**config**).

```
Console#!2
Console#config
Console(config)#
```

reload

Use this command to restart the system.

Note: When the system is restarted, it will always run the Power-On Self-Test. It will also retain all configuration information stored in non-volatile memory by the **copy running-config startup-config** command.

Default Setting

None

Command Mode

Privileged Exec

Command Usage

This command resets the entire system.

Example

This example shows how to reset the switch:

```
Console#reload
System will be restarted, continue <y/n>? y
```

end

Use this command to return to Privileged Exec mode.

Default Setting

None

Command Mode

Global Configuration, Interface Configuration, Line Configuration,
VLAN Database Configuration, Router Configuration

Example

This example shows how to return to the Privileged Exec mode from the Interface Configuration mode:

```
Console(config-if)#end
Console#
```

exit

Use this command to return to the previous configuration mode or exit the configuration program.

Default Setting

None

Command Mode

Any

Example

This example shows how to return to the Privileged Exec mode from the Global Configuration mode, and then quit the CLI session:

```
Console(config)#exit
Console#exit

Press ENTER to start session

User Access Verification

Username:
```

quit

Use this command to exit the configuration program.

Default Setting

None

Command Mode

Normal Exec, Privileged Exec

Command Usage

The quit and exit commands can both exit the configuration program.

Example

This example shows how to quit a CLI session:

```
Console#quit

Press ENTER to start session

User Access Verification

Username:
```

System Management Commands

These commands are used to control system logs, passwords, user names, browser configuration options, and display or configure a variety of other system information.

Command Group	Function	Page
Device Designation	Configures information that uniquely identifies this switch	4-31
User Access	Configures the basic user names and passwords for management access	4-32
Web Server	Enables management access via a Web browser	4-35
Event Logging	Controls logging of error messages	4-37
Time (System Clock)	Sets the system clock using SNTP and time zone commands	4-41
System Status	Displays system configuration, active managers, and version information	4-47

Device Designation Commands

Command	Function	Mode	Page
hostname	Specifies the host name for the switch	GC	4-32
snmp-server contact	Sets the system contact string	GC	4-91
snmp-server location	Sets the system location string	GC	4-92

hostname

Use this command to specify or modify the host name for this device. Use the **no** form to restore the default host name.

Syntax

hostname *name*
no hostname
name - The name of this host. (Maximum length: 255 characters)

Default Setting

None

Command Mode

Global Configuration

Example

```
Console(config)#hostname SMC6724L3
Console(config)#
```

User Access Commands

The basic commands required for management access are listed in this section. This switch also includes other options for password checking via the console or a Telnet connection (page 4-13), user authentication via a remote authentication server (page 4-60), and host access authentication for specific ports (page 4-66).

Command	Function	Mode	Page
username	Establishes a user name-based authentication system at login	GC	4-33
enable password	Sets a password to control access to the Privileged Exec level	GC	4-34

username

Use this command to add named users, require authentication at login, specify or change a user's password (or specify that no password is required), or specify or change a user's access level. Use the **no** form to remove a user name.

Syntax

username *name* {**access-level** *level* | **nopassword** |
password {**0** | **7**} *password*}

no username *name*

- *name* - The name of the user.
(Maximum length: 8 characters, case sensitive. Maximum users: 16)
- **access-level** *level* - Specifies the user level.
The device has two predefined privilege levels:
0: Normal Exec, **15**: Privileged Exec.
- **nopassword** - No password is required for this user to log in.
- {**0** | **7**} - **0** means plain password, **7** means encrypted password.
- **password** *password* - The authentication password for the user.
(Maximum length: 8 characters plain text, 32 encrypted, case sensitive)

Default Setting

- The default access level is Normal Exec.
- The factory defaults for the user names and passwords are:

username	access-level	password
guest	0	guest
admin	15	admin

Command Mode

Global Configuration

Command Usage

The encrypted password is required for compatibility with legacy password settings (i.e., plain text or encrypted) when reading the configuration file during system bootup or when downloading the configuration file from a TFTP server. There is no need for you to manually configure encrypted passwords.

Example

This example shows how to set the access level and password for a user.

```
Console(config)#username bob access-level 15
Console(config)#username bob password 0 smith
Console(config)#
```

enable password

After initially logging onto the system, you should set the Privileged Exec password. Remember to record it in a safe place. Use this command to control access to the Privileged Exec level from the Normal Exec level. Use the **no** form to reset the default password.

Syntax

enable password [*level level*] {**0** | **7**} *password*

no enable password [*level level*]

- **level level** - Level 15 for Privileged Exec. (Levels 0-14 are not used.)
- {**0** | **7**} - 0 means plain password, 7 means encrypted password.
- *password* - password for this privilege level.
(Maximum length: 8 characters plain text, 32 encrypted, case sensitive)

Default Setting

- The default is level 15.
- The default password is “super”

Command Mode

Global Configuration

Command Usage

- You cannot set a null password. You will have to enter a password to change the command mode from Normal Exec to Privileged Exec with the **enable** command (page 4-25).
- The encrypted password is required for compatibility with legacy password settings (i.e., plain text or encrypted) when reading the configuration file during system bootup or when downloading the configuration file from a TFTP server. There is no need for you to manually configure encrypted passwords.

Example

```
Console(config)#enable password level 15 0 admin
Console(config)#
```

Related Commands

enable (4-25)

Web Server Commands

Command	Function	Mode	Page
ip http port	Specifies the port to be used by the Web browser interface	GC	4-35
ip http server	Allows the switch to be monitored or configured from a browser	GC	4-36

ip http port

Use this command to specify the TCP port number used by the Web browser interface. Use the **no** form to use the default port.

Syntax

ip http port *port-number*

no ip http port

port-number - The TCP port to be used by the browser interface.
(Range: 1-65535)

Default Setting

80

Command Mode

Global Configuration

Example

```
Console(config)#ip http port 769
Console(config)#
```

Related Commands

ip http server (4-36)

ip http server

Use this command to allow this device to be monitored or configured from a browser. Use the **no** form to disable this function.

Syntax

ip http server
no ip http server

Default Setting

Enabled

Command Mode

Global Configuration

Example

```
Console(config)#ip http server
Console(config)#
```

Related Commands

ip http port (4-35)

Event Logging Commands

Command	Function	Mode	Page
logging on	Controls logging of error messages	GC	4-37
logging history	Limits syslog messages saved to switch memory based on severity	GC	4-38
clear logging	Clears messages from the logging buffer	PE	4-39
show logging	Displays the state of logging	PE	4-40

logging on

Use this command to control logging of error messages. This command sends debug or error messages to switch memory. The **no** form disables the logging process.

Syntax

logging on
no logging on

Default Setting

None

Command Mode

Global Configuration

Command Usage

The logging process controls error messages saved to switch memory. You can use the logging history command to control the type of error messages that are stored.

Example

```
Console(config)#logging on
Console(config)#
```

Related Commands

logging history (4-38)
clear logging (4-39)

logging history

Use this command to limit syslog messages saved to switch memory based on severity. The **no** form returns the logging of syslog messages to the default level.

Syntax

```
logging history {flash | ram} level
no logging history {flash | ram}
```

- **flash** - Event history stored in flash memory (i.e., permanent memory).
- **ram** - Event history stored in temporary RAM (i.e., memory flushed on power reset).
- *level* - One of the level arguments listed below. Messages sent include the selected level down to level 0.

Level Argument	Level	Description
debugging	7	Debugging messages
informational	6	Informational messages only
notifications	5	Normal but significant condition, such as cold start
warnings	4	Warning conditions (e.g., return false, unexpected return)
errors	3	Error conditions (e.g., invalid input, default used)
critical	2	Critical conditions (e.g., memory allocation, or free memory error - resource exhausted)
alerts	1	Immediate action needed
emergencies	0	System unusable

* There are only Level 2, 5 and 6 error messages for the current firmware release.

Default Setting

Flash: errors (level 3 - 0)
RAM: warnings (level 7 - 0)

Command Mode

Global Configuration

Command Usage

The message level specified for flash memory must be a higher priority (i.e., numerically lower) than that specified for RAM.

Example

```
Console(config)#logging history ram 0
Console(config)#
```

clear logging

Use this command to clear messages from the log buffer.

Syntax

clear logging [**flash** | **ram**]

- **flash** - Event history stored in flash memory (i.e., permanent memory).
- **ram** - Event history stored in temporary RAM (i.e., memory flushed on power reset).

Default Setting

Flash and RAM

Command Mode

Privileged Exec

Example

```
Console#clear logging
Console#
```

Related Commands

show logging (4-40)

show logging

Use this command to display the logging configuration, along with any system and event messages stored in memory.

Syntax

show logging {flash | ram}

- **flash** - Event history stored in flash memory (i.e., permanent memory).
- **ram** - Event history stored in temporary RAM (i.e., memory flushed on power reset).

Default Setting

None

Command Mode

Privileged Exec

Command Usage

This command shows the following information:

- Syslog logging – Whether or not system logging has been enabled via the **logging on** command.
- History logging in FLASH/RAM – The message level(s) that are reported based on the **logging history** command.
- Any system and event messages stored in memory.

Example

The following example shows that system logging is enabled, the message level for flash memory is “errors” (i.e., default level 3 - 0), the message level for RAM is “debugging” (i.e., default level 7 - 0), and lists one sample error

```

Console#show logging flash
Syslog logging: Enable
History logging in FLASH: level errors
[0] 0:0:5 1/1/1
    "PRI_MGR_InitDefault function fails."
      level: 3, module: 13, function: 0, and event no.: 0
Console#show logging ram
Syslog logging: Enable
History logging in RAM: level debugging
[0] 0:0:5 1/1/1
    "PRI_MGR_InitDefault function fails."
      level: 3, module: 13, function: 0, and event no.: 0
Console#

```

Time Commands

The system clock can be dynamically set by polling a set of specified time servers (NTP or SNTP), or by using information broadcast by local time servers.

Command	Function	Mode	Page
sntp client	Accepts time from specified time servers	GC	4-42
sntp server	Specifies one or more time servers	GC	4-43
sntp poll	Sets the interval at which the client polls for time	GC	4-44
sntp broadcast client	Accepts time from any time broadcast server	GC	4-45
show sntp	Shows current SNTP configuration settings	NE, PE	4-45
clock timezone	Sets the time zone for the switch's internal clock	GC	4-46

sntp client

Use this command to enable SNTP client requests for time synchronization from NTP or SNTP time servers specified with the **sntp servers** command. Use the **no** form of this command to disable SNTP client requests.

Syntax

sntp client
no sntp client

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

- The time acquired from time servers is used to record accurate dates and times for log events. Without SNTP, the switch only records the time starting from the factory default set at the last bootup (i.e., 00:00:00, Jan. 1, 2001).
- This command enables client time requests to time servers specified via the **sntp servers** command. It issues time synchronization requests based on the interval set via the **sntp poll** command.
- The SNTP time query method is set to client mode when the first **sntp client** command is issued. However, if the **sntp broadcast client** command is issued, then the **no sntp broadcast client** command must be used to return the switch to SNTP client mode.

Example

```

Console(config)#ntp server 10.1.0.19
Console(config)#ntp poll 60
Console(config)#ntp client
Console(config)#end
Console#show ntp
Current time: Dec 23 02:52:44 2002
Poll interval: 60
Current mode: unicast
Console#

```

Related Commands

ntp server (4-43)
 ntp poll (4-44)
 ntp broadcast client (4-45)
 show ntp (4-45)

ntp server

Use this command to set the IP address of the servers to which SNTP time requests are issued. Use the this command with no arguments to clear all time servers from the current list.

Syntax

ntp server [*ip1* [*ip2* [*ip3*]]]

ip - IP address of an time server (NTP or SNTP).
 (Range: 1 - 3 addresses)

Default Setting

None

Command Mode

Global Configuration

Command Usage

This command specifies time servers from which the switch will poll for time updates when set to SNTP client mode. The client will poll the time servers in the order specified until a response is received. It issues time synchronization requests based on the interval set via the `sntp poll` command.

Example

```
Console(config)#sntp server 10.1.0.19
Console#
```

Related Commands

- sntp client (4-42)
- sntp poll (4-44)
- show sntp (4-45)

sntp poll

Use this command to set the interval between sending time requests when the switch is set to SNTP client mode. Use the **no** form to restore to the default.

Syntax

sntp poll *seconds*
no sntp poll

seconds - Interval between time requests. (Range: 16-16384 seconds)

Default Setting

16 seconds

Command Mode

Global Configuration

Command Usage

This command is only applicable when the switch is set to SNTP client mode.

Example

```
Console(config)#sntp poll 60
Console#
```

Related Commands

sntp client (4-42)

sntp broadcast client

Use this command to synchronize the switch's clock based on time broadcast from time servers (using the multicast address 224.0.1.1). Use the **no** form to disable SNTP broadcast client mode.

Syntax

sntp broadcast client
no sntp broadcast client

Default Setting

Disabled

Command Mode

Global Configuration

Example

```
Console(config)#sntp broadcast client
Console#
```

show sntp

Use this command to display the current time and configuration settings for the SNTP client, and whether or not the local time has been properly updated.

Command Mode

Normal Exec, Privileged Exec

Command Usage

This command displays the current time, the poll interval used for sending time synchronization requests (when the switch is set to SNTP client mode), and the current SNTP mode (i.e., client or broadcast).

Example

```
Console#show sntp
Current time:  Dec 23 05:13:28 2002
Poll interval: 16
Current mode:  unicast
Console#
```

clock timezone

Use this command to set the time zone for the switch's internal clock.

Syntax

clock timezone *name* **hour** *hours* **minute** *minutes* {**before-utc** | **after-utc**}

- *name* - Name of timezone, usually an acronym. (Range: 1-29 characters)
- *hours* - Number of hours before/after UTC. (Range: 1-12 hours)
- *minutes* - Number of minutes before/after UTC. (Range: 0-59 minutes)
- **before-utc** - Sets the local time zone before (east) of UTC.
- **after-utc** - Sets the local time zone after (west) of UTC.

Default Setting

None

Command Mode

Global Configuration

Command Usage

This command sets the local time zone relative to the Coordinated Universal Time (UTC, formerly Greenwich Mean Time or GMT), based on the earth's prime meridian, zero degrees longitude. To display

a time corresponding to your local time, you must indicate the number of hours and minutes your time zone is east (before) or west (after) of UTC.

Example

```
Console(config)#clock timezone Japan hours 8 minute 0 after-UTC
Console(config)#
```

Related Commands

show snmp (4-45)

System Status Commands

Command	Function	Mode	Page
show startup-config	Displays the contents of the configuration file (stored in flash memory) that is used to start up the system	PE	4-47
show running-config	Displays the configuration data currently in use	PE	4-49
show system	Displays system information	NE, PE	4-51
show users	Shows all active console and Telnet sessions, including user name, idle time, and IP address of Telnet clients	NE, PE	4-51
show version	Displays version information for the system	NE, PE	4-52

show startup-config

Use this command to display the configuration file stored in non-volatile memory that is used to start up the system.

Default Setting

None

Command Mode

Privileged Exec

Command Usage

- Use this command in conjunction with the **show running-config** command to compare the information in running memory to the information stored in non-volatile memory.
- This command displays settings for key command modes. Each mode group is separated by “!” symbols, and includes the configuration mode command, and corresponding commands. This command displays the following information:
 - SNMP community strings
 - Users (names and access levels)
 - VLAN database (VLAN ID, name and state)
 - VLAN configuration settings for each interface
 - IP address configured for VLANs
 - Routing protocol configuration settings
 - Spanning tree settings
 - Any configured settings for the console port and Telnet

Example

```
Console#show startup-config
building startup-config, please wait.....
!
!
username admin access-level 15
username admin password 0 admin
!
username guest access-level 0
username guest password 0 guest
!
enable password level 15 0 super
!
snmp-server community public ro
snmp-server community private rw
!
vlan database
  vlan 1 name DefaultVlan media ethernet state active
!
!
interface ethernet 1/1
  switchport allowed vlan add 1 untagged
  switchport native vlan 1
.
.
.
```

```
interface vlan 1
ip address 0.0.0.0 255.0.0.0
ip address dhcp
!
line console
!
line vty
!
end
Console#
```

Related Commands

show running-config (4-49)

show running-config

Use this command to display the configuration information currently in use.

Default Setting

None

Command Mode

Privileged Exec

Command Usage

- Use this command in conjunction with the **show running-config** command to compare the information in running memory to the information stored in non-volatile memory.
- This command displays settings for key command modes. Each mode group is separated by “!” symbols, and includes the configuration mode command, and corresponding commands. This command displays the following information:
 - SNMP community strings
 - Users (names, access levels, and encrypted passwords)
 - VLAN database (VLAN ID, name and state)
 - VLAN configuration settings for each interface
 - IP address configured for VLANs

- Routing protocol configuration settings
- Spanning tree settings
- Any configured settings for the console port and Telnet

Example

```
Console#show running-config
building running-config, please wait.....
!
!
snmp-server community private rw
snmp-server community public ro
!
!
username admin access-level 15
username admin password 7 21232f297a57a5a743894a0e4a801fc3
username guest access-level 0
username guest password 7 084e0343a0486ff05530df6c705c8bb4
enable password level 15 7 1b3231655cebb7a1f783eddf27d254ca
!
vlan database
vlan 1 name DefaultVlan media ethernet state active
!
!
interface ethernet 1/1
switchport allowed vlan add 1 untagged
switchport native vlan 1
.
.
.
!
interface vlan 1
ip address 10.1.0.1 255.255.255.0
!
!
!
!
line console
!
line vty
!
end
Console#
```

Related Commands

show startup-config (4-47)

show system

Use this command to display system information.

Default Setting

None

Command Mode

Normal Exec, Privileged Exec

Command Usage

- For a description of the items shown by this command, refer to “Displaying System Information” on page -12.
- The POST results should all display “PASS.” If any POST test indicates “FAIL,” contact your distributor for assistance.

Example

```
Console#show system
System description: TigerSwitch 10/100 Managed 24+2 L3 Switch
System OID string: 1.3.6.1.4.1.202.20.29
System information
System Up time: 0 days, 1 hours, 23 minutes, and 44.61 seconds
System Name       : [NONE]
System Location   : [NONE]
System Contact    : [NONE]
MAC address       : 00-30-f1-47-58-3a
Web server        : enable
Web server port   : 80
Ingress rate limit : Disabled
POST result
Console#
```

show users

Shows all active console and Telnet sessions, including user name, idle time, and IP address of Telnet client.

Default Setting

None

Command Mode

Normal Exec, Privileged Exec

Command Usage

The session used to execute this command is indicated by a “*” symbol next to the Line (i.e., session) index number.

Example

```
Console#show users
Username accounts:
Username Privilege
-----
    guest          0
    admin          15

Online users:
Line      Username Idle time (h:m:s) Remote IP addr.
-----
* 0   console   admin          0:00:00
    1   vty 0    admin          0:04:37      10.1.0.19

Console#
```

show version

Use this command to display hardware and software version information for the system.

Default Setting

None

Command Mode

Normal Exec, Privileged Exec

Command Usage

See “Displaying Switch Hardware/Software Versions” on page -14 for detailed information on the items displayed by this command.

Example

```

Console#show version
Unit1
  Serial number      :1111111111
  Service tag        :
  Hardware version    :R0A
  Number of ports     :26
  Main power status   :up
  Redundant power status :not present
Agent(master)
  Unit id            :1
  Loader version      :1.0.0.0
  Boot rom version    :1.0.0.0
  Operation code version :1.0.1.3
Console#

```

Flash/File Commands

These commands are used to manage the system code or configuration files.

Command	Function	Mode	Page
copy	Copies a code image or a switch configuration to or from flash memory or a TFTP server	PE	4-53
delete	Deletes a file or code image	PE	4-56
dir	Displays a list of files in flash memory	PE	4-57
whichboot	Displays the files booted	PE	4-58
boot system	Specifies the file or image used to start up the system	GC	4-59

copy

Use this command to move (upload/download) a code image or configuration file between the switch's flash memory and a TFTP server. When you save the system code or configuration settings to a file on a TFTP server, that file can later be downloaded to the switch to restore system operation. The success of the file transfer depends on the accessibility of the TFTP server and the quality of the network connection.

Syntax

```
copy file {file | running-config | startup-config | tftp}  
copy running-config {file | startup-config | tftp}  
copy startup-config {file | running-config | tftp}  
copy tftp {file | running-config | startup-config}
```

- **file** - Keyword that allows you to copy to/from a file.
- **running-config** - Keyword that allows you to copy to/from the current running configuration.
- **startup-config** - The configuration used for system initialization.
- **tftp** - Keyword that allows you to copy to/from a TFTP server.

Default Setting

None

Command Mode

Privileged Exec

Command Usage

- The system prompts for data required to complete the copy command.
- The destination file name should not contain slashes (\ or /), the leading letter of the file name should not be a period (.), and the maximum length for file names on the TFTP server is 127 characters or 31 characters for files on the switch. (Valid characters: A-Z, a-z, 0-9, “.”, “-”, “_”)
- Due to the size limit of the flash memory, the switch supports only two operation code files.
- The maximum number of user-defined configuration files depends on available memory.
- You can use “Factory_Default_Config.cfg” as the source to copy from the factory default configuration file, but you cannot use it as the destination.
- To replace the startup configuration, you must use **startup-config** as the destination.
- The Boot ROM and Loader cannot be uploaded or downloaded from the TFTP server. You must use a direct console connection and access

the download menu during a boot up to download the Boot ROM (or diagnostic) image. See “Upgrading Firmware via the Serial Port” on page B-1 for more details.

Example

The following example shows how to upload the configuration settings to a file on the TFTP server:

```
Console#copy file tftp
Choose file type:
  1. config:  2. opcode: <1-2>: 1
Source file name: startup
TFTP server ip address: 10.1.0.99
Destination file name: startup.01
TFTP completed.
Success.
Console#
```

The following example shows how to copy the running configuration to a startup file.

```
Console#copy running-config file
destination file name : startup
Write to FLASH Programming.
\Write to FLASH finish.
Success.
Console#
```

The following example shows how to download a configuration file:

```
Console#copy tftp startup-config
TFTP server ip address: 10.1.0.99
Source configuration file name: startup.01
Startup configuration file name [startup]:
Write to FLASH Programming.

\Write to FLASH finish.
Success.
Console#
```

delete

Use this command to delete a file or image.

Syntax

delete *filename*

filename - Name of the configuration file or image name.

Default Setting

None

Command Mode

Privileged Exec

Command Usage

- If the file type is used for system startup, then this file cannot be deleted.
- “Factory_Default_Config.cfg” cannot be deleted.

Example

This example shows how to delete the test2.cfg configuration file from flash memory.

```
Console#delete test2.cfg
Console#
```

Related Commands

dir (4-57)

dir

Use this command to display a list of files in flash memory.

Syntax

dir [**boot-rom** | **config** | **opcode** [:*filename*]]

The type of file or image to display includes:

- **boot-rom** - Boot ROM (or diagnostic) image file.
- **config** - Switch configuration file.
- **opcode** - Run-time operation code image file.
- *filename* - Name of the file or image. If this file exists but contains errors, information on this file cannot be shown.

Default Setting

None

Command Mode

Privileged Exec

Command Usage

- If you enter the command **dir** without any parameters, the system displays all files.
- File information is shown below:

Column Heading	Description
file name	The name of the file.
file type	File types: Boot-Rom, Operation Code, and Config file.
startup	Shows if this file is used when the system is started.
size	The length of the file in bytes.

Example

The following example shows how to display all file information:

Console#dir				
	file name	file type	startup	size (byte)
	diag_0060	Boot-Rom image	Y	111360
	run_01642	Operation Code	N	1074304
	run_0200	Operation Code	Y	1083008
	Factory_Default_Config.cfg	Config File	N	2574
	startup	Config File	Y	2710
Total free space:				0
Console#				

whichboot

Use this command to display which files were booted when the system powered up.

Default Setting

None

Command Mode

Privileged Exec

Example

This example shows the information displayed by the **whichboot** command. See the table under the **dir** command for a description of the file information displayed by this command.

Console#whichboot				
	file name	file type	startup	size (byte)
	diag_0060	Boot-Rom image	Y	111360
	run_0200	Operation Code	Y	1083008
	startup	Config File	Y	2710
Console#				

boot system

Use this command to specify the file or image used to start up the system.

Syntax

boot system {**boot-rom** | **config** | **opcode**}: *filename*

The type of file or image to set as a default includes:

- **boot-rom** - Boot ROM.
- **config** - Configuration file.
- **opcode** - Run-time operation code.

The colon (:) is required.

- *filename* - Name of the configuration file or image name.

Default Setting

None

Command Mode

Global Configuration

Command Usage

- A colon (:) is required after the specified file type.
- If the file contains an error, it cannot be set as the default file.

Example

```
Console(config)#boot system config: startup
Console(config)#
```

Related Commands

dir (4-57)
whichboot (4-58)

Authentication Commands

You can configure this switch to authenticate users logging into the system for management access using local or RADIUS authentication methods. You can also enable port-based authentication for network client access using IEEE 802.1x.

Command Group	Function	Page
Authentication Sequence	Defines logon authentication method and precedence	4-60
RADIUS Client	Configures settings for authentication via a remote server	4-62
Port Authentication	Configures host authentication on specific ports using 802.1x	4-67

Authentication Sequence

Command	Function	Mode	Page
authentication login	Defines logon authentication method and precedence	GC	4-60

authentication login

Use this command to define the login authentication method and precedence. Use the **no** form to restore the default.

Syntax

authentication login {[local] [radius]}

no authentication login

- **local** - Use local password only.
- **radius** - Use RADIUS server password only.

Default Setting

Local

Command Mode

Global Configuration

Command Usage

- RADIUS uses UDP which only offers best effort delivery. Also, note that RADIUS encrypts only the password in the access-request packet from the client to the server.
- RADIUS logon authentication assigns a specific privilege level for each user name and password pair. The user name, password, and privilege level must be configured on the authentication server.
- You can specify two authentication methods in a single command to indicate the authentication sequence. For example, if you enter “**authentication login radius local**,” the user name and password on the RADIUS server is verified first. If the RADIUS server is not available, then the local user name and password is checked.

Example

```
Console(config)#authentication login radius
Console(config)#
```

Related Commands

username - for setting the local user names and passwords (4-33)

RADIUS Client

Remote Authentication Dial-in User Service (RADIUS) is a logon authentication protocol that uses software running on a central server to control access to RADIUS-aware devices on the network. An authentication server contains a database of multiple user name/password pairs with associated privilege levels for each user or group that require management access to a switch.

Command	Function	Mode	Page
radius-server host	Specifies the RADIUS server	GC	4-62
radius-server port	Sets the RADIUS server network port	GC	4-63
radius-server key	Sets the RADIUS encryption key	GC	4-63

Command	Function	Mode	Page
radius-server retransmit	Sets the number of retries	GC	4-64
radius-server timeout	Sets the interval between sending authentication requests	GC	4-65
show radius-server	Shows the current RADIUS settings	PE	4-65

radius-server host

Use this command to specify the RADIUS server. Use the **no** form to restore the default.

Syntax

radius-server host *host_ip_address*

no radius-server host

host_ip_address - IP address of server.

Default Setting

10.1.0.1

Command Mode

Global Configuration

Example

```
Console(config)#radius-server host 192.168.1.25
Console(config)#
```

radius-server port

Use this command to set the RADIUS server network port. Use the **no** form to restore the default.

Syntax

radius-server port *port_number*

no radius-server port

port_number - RADIUS server UDP port used for authentication messages. (Range: 1-65535)

Default Setting

1812

Command Mode

Global Configuration

Example

```
Console(config)#radius-server port 181
Console(config)#
```

radius-server key

Use this command to set the RADIUS encryption key. Use the **no** form to restore the default.

Syntax

radius-server key *key_string*

no radius-server key

key_string - Encryption key used to authenticate logon access for client. Do not use blank spaces in the string. (Maximum length: 20 characters)

Default Setting

None

Command Mode

Global Configuration

Example

```
Console(config)#radius-server key green
Console(config)#
```

radius-server retransmit

Use this command to set the number of retries. Use the **no** form to restore the default.

Syntax

radius-server retransmit *number_of_retries*
no radius-server retransmit

number_of_retries - Number of times the switch will try to authenticate logon access via the RADIUS server. (Range: 1 - 30)

Default Setting

2

Command Mode

Global Configuration

Example

```
Console(config)#radius-server retransmit 5
Console(config)#
```

radius-server timeout

Use this command to set the interval between transmitting authentication requests to the RADIUS server. Use the **no** form to restore the default.

Syntax

radius-server timeout *number_of_seconds*

no radius-server timeout

number_of_seconds - Number of seconds the switch waits for a reply before resending a request. (Range: 1-65535)

Default Setting

5

Command Mode

Global Configuration

Example

```
Console(config)#radius-server timeout 10
Console(config)#
```

show radius-server

Use this command to display the current settings for the RADIUS server.

Default Setting

None

Command Mode

Privileged Exec

Example

```
Console#show radius-server
Server IP address: 10.1.0.1
Communication key with radius server:
Server port number: 1812
Retransmit times: 2
Request timeout: 5
Console#
```

802.1x Port Authentication

The switch supports IEEE 802.1x (dot1x) port-based access control that prevents unauthorized access to the network by requiring users to first enter a user ID and password for authentication. Client authentication is controlled centrally by a RADIUS server using EAPOL (Extensible Authentication Protocol Over LAN).

Command	Function	Mode	Page
authentication dot1x default	Sets the default authentication server type	GC	4-67
dot1x default	Resets all dot1x parameters to their default values	GC	4-67
dot1x max-req	Sets the maximum number of times the switch will attempt to send a request to the RADIUS server before authentication fails	GC	4-68
dot1x port-control	Sets dot1x mode for a port interface	IC	4-68
dot1x re-authenticate	Forces re-authentication on specific ports	PE	4-69
dot1x re-authentication	Enables re-authentication for all ports	GC	4-69
dot1x timeout quiet-period	Sets the time that a switch port waits after the Max Request Count has been exceeded before attempting to acquire a new client	GC	4-70
dot1x timeout re-authperiod	Sets the time period after which a connected client must be re-authenticated	GC	4-70
dot1x timeout tx-period	Sets the time period during an authentication session that the switch waits before re-transmitting an EAP packet	GC	4-71
show dot1x	Shows all dot1x related information	PE	4-72

authentication dot1x default

Sets the default authentication server type. Use the **no** form to restore the default.

Syntax

authentication dot1x default radius
no authentication dot1x

Default Setting

RADIUS

Command Mode

Global Configuration

Example

```
Console(config)#authentication dot1x default radius
Console(config)#
```

dot1x default

Sets all configurable dot1x global and port settings to their default values.

Syntax

dot1x default

Command Mode

Global Configuration

Example

```
Console(config)#dot1x default
Console(config)#
```

dot1x max-req

Sets the maximum number of times the switch port will retransmit an EAP request packet to the client before it times out the authentication session. Use the **no** form to restore the default.

Syntax

dot1x max-req *count*
no dot1x max-req

count – The maximum number of requests (Range: 1-10)

Default

2

Command Mode

Global Configuration

Example

```
Console(config)#dot1x max-req 2
Console(config)#
```

dot1x port-control

Sets the dot1x mode on a port interface. Use the **no** form to restore the default.

Syntax

dot1x port-control {**auto** | **force-authorized** | **force-unauthorized**}
no dot1x port-control

- **auto** – Requires a dot1x-aware connected client to be authorized by the RADIUS server. Clients that are not dot1x-aware will be denied access.
- **force-authorized** – Configures the port to grant access to all clients, either dot1x-aware or otherwise.
- **force-unauthorized** – Configures the port to deny access to all clients, either dot1x-aware or otherwise.

Default

force-authorized

Command Mode

Interface Configuration

Example

```
Console(config)#interface eth 1/2
Console(config-if)#dot1x port-control auto
Console(config-if)#
```

dot1x re-authenticate

Forces re-authentication on all ports or a specific interface.

Syntax

dot1x re-authenticate [*interface*]

interface

- **ethernet** *unit/port*
 - *unit* - This is device 1.
 - *port* - Port number.

Command Mode

Privileged Exec

Example

```
Console#dot1x re-authenticate
Console#
```

dot1x re-authentication

Enables periodic re-authentication globally for all ports. Use the **no** form to disable re-authentication.

Syntax

dot1x re-authentication

no dot1x re-authentication

Command Mode

Global Configuration

Example

```
Console(config)#dot1x re-authentication
Console(config)#
```

dot1x timeout quiet-period

Sets the time that a switch port waits after the Max Request Count has been exceeded before attempting to acquire a new client. Use the **no** form of this command to reset the default.

Syntax

dot1x timeout quiet-period *seconds*

no dot1x timeout quiet-period *seconds*

seconds - The number of seconds. (Range: 1-65535)

Default

60 seconds

Command Mode

Global Configuration

Example

```
Console(config)#dot1x timeout quiet-period 350
Console(config)#
```

dot1x timeout re-authperiod

Sets the time period after which a connected client must be re-authenticated.

Syntax

dot1x timeout re-authperiod *seconds*

no dot1x timeout re-authperiod

seconds - The number of seconds. (Range: 1-65535)

Default

3600 seconds

Command Mode

Global Configuration

Example

```
Console(config)#dot1x timeout re-authperiod 300
Console(config)#
```

dot1x timeout tx-period

Sets the time that the switch waits during an authentication session before re-transmitting an EAP packet. Use the **no** form to reset to the default value.

Syntax

dot1x timeout tx-period *seconds*

no dot1x timeout tx-period

seconds - The number of seconds. (Range: 1-65535)

Default

30 seconds

Command Mode

Global Configuration

Example

```
Console(config)#dot1x timeout tx-period 300
Console(config)#
```

show dot1x

Use this command to show general port authentication related settings on the switch or a specific interface.

Syntax

show dot1x [**statistics**] [**interface** *interface*]

interface

- **ethernet** *unit/port*
 - *unit* - This is device 1.
 - *port* - Port number.

Command Mode

Privileged Exec

Command Usage

This command displays the following information:

- *Global 802.1X Parameters* – Displays the global port access control parameters that can be configured for this switch as described in the preceding pages, including reauth-enabled (page 4-69), reauth-period (page 4-70), quiet-period (page 4-70), tx-period (page 4-71), and max-req (page 4-68). It also displays the following global parameters which are set to a fixed value, including the following items:
 - *supp-timeout*– Supplicant timeout.
 - *server-timeout*– Server timeout.
 - *reauth-max*– Maximum number of reauthentication attempts.
- *802.1X Port Summary* – Displays the port access control parameters for each interface, including the following items:
 - *Status*– Administrative state for port access control.
 - *Mode*– Dot1x port control mode (page 4-68).
 - *Authorized*– Authorization status (yes or n/a - not authorized).
- *802.1X Port Details* – Displays detailed port access control settings for each interface as described in the preceding pages, including administrative status for port access control, Max request (page 4-68), Quiet period (page 4-70), Reauth period (page 4-70), Tx period

(page 4-71), and Port-control (page 4-68). It also displays the following information:

- Status— Authorization status (authorized or unauthorized).
- Supplicant— MAC address of authorized client.
- *Authenticator State Machine*
 - State— Current state (including initialize, disconnected, connecting, authenticating, authenticated, aborting, held, force_authorized, force_unauthorized).
 - Reauth Count— Number of times connecting state is re-entered.
- *Backend State Machine*
 - State— Current state (including request, response, success, fail, timeout, idle, initialize).
 - Request Count— Number of EAP Request packets sent to the Supplicant without receiving a response.
 - Identifier(Server)— Identifier carried in the most recent EAP Success, Failure or Request packet received from the Authentication Server.
- *Reauthentication State Machine*
 - State— Current state (including initialize, reauthenticate).

Example

```

Console#show dot1x
Global 802.1X Parameters
reauth-enabled: yes
reauth-period: 300
quiet-period: 350
tx-period: 300
supp-timeout: 30
server-timeout: 30
reauth-max: 2
max-req: 2

```

802.1X Port Summary

Port	Name	Status	Mode	Authorized
1		disabled	ForceAuthorized	n/a
2		disabled	ForceAuthorized	n/a
:				
25		disabled	ForceAuthorized	yes
26		enabled	Auto	yes

```
802.1X Port Details

802.1X is disabled on port 1
:
802.1X is enabled on port 26
Max request      2
Quiet period     350
Reauth period    300
Tx period        300
Status           Unauthorized
Port-control     Auto
Supplicant       00-00-00-00-00-00

Authenticator State Machine
State            Connecting
Reauth Count     3
Backend State Machine
State            Idle
Request Count    0
Identifier(Server) 0

Reauthentication State Machine
State            Initialize
Console#
```

Access Control List Commands

Access Control Lists (ACL) provide packet filtering for IP frames (based on address, protocol, TCP/UDP port number or TCP control code) or non-IP frames (based on MAC address or Ethernet type). To filter incoming packets, first create an access list, add the required rules, and then bind the list to a specific port.

An ACL is a sequential list of permit or deny conditions that apply to IP addresses, MAC addresses, or other more specific criteria. This switch tests incoming packets against the conditions in an ACL one by one. If a list contains all permit rules, a packet will be accepted as soon as it passes any of the rules. If a list contains all deny rules, then a packet will be rejected as soon as it fails any one of the rules. In other words, if no rules match for a permit list, the packet is dropped; and if no rules match for a deny list, the packet is accepted.

There are three filtering modes:

- Standard IP ACL mode (STD-ACL) filters packets based on the source IP address.
- Extended IP ACL mode (EXT-ACL) filters packets based on source or destination IP address, as well as protocol type and TCP/UDP port number. If the TCP protocol type is specified, then you can also filter packets based on the TCP control code.
- MAC ACL mode (MAC-ACL) filters packets based on the source or destination MAC address and the Ethernet frame type (RFC 1060).

The following restrictions apply to ACLs:

- Each ACL can have up to 32 rules.
- The maximum number of ACLs is also 32.
- However, due to resource restrictions, the average number of rules bound to the ports should not exceed 20.
- The switch does not support the explicit “deny any any” rule for the IP ACL or MAC ACL. If these rules are included in an ACL, and you attempt to bind the ACL to an interface, the bind operation will fail.
- An access list can only contain all permit rules or all deny rules. In other words, for performance reasons, you cannot mix permit and deny rules in the same list.

The order in which active ACLs are checked is as follows:

1. User-defined rules in the MAC ACL.
2. User-defined rules in the IP ACL.
3. Explicit default rule (permit any any) in the IP ACL.
4. Explicit default rule (permit any any) in the MAC ACL.
5. If no explicit rule is matched, the implicit default is permit all.

Command Groups	Function	Page
IP ACLs	Configures ACLs based on IP addresses, TCP/UDP port number, protocol type, and TCP control code	4-76
MAC ACLs	Configures ACLs based on hardware addresses, packet format, and Ethernet type	4-84
ACL Information	Displays ACLs and associated rules; shows ACLs assigned to each port	4-89

IP ACLs

Command	Function	Mode	Page
access-list ip	Creates an IP ACL and enters configuration mode	GC	4-76
permit, deny	Filters packets matching a specified source IP address	STD-ACL	4-78
permit, deny	Filters packets meeting the specified criteria, including source and destination IP address, TCP/UDP port number, protocol type, and TCP control code	EXT-ACL	4-79
ip access-group	Adds a port to an IP ACL	IC	4-81
show ip access-group	Shows port assignments for IP ACLs	PE	4-81
show ip access-list	Displays the rules for configured IP ACLs	PE	4-83

access-list ip

Use this command to add an IP access list and enter configuration mode for standard or extended IP ACLs. Use the **no** form to remove the specified ACL.

Syntax

```
access-list ip {standard | extended} acl_name
no access-list ip {standard | extended} acl_name
```

- **standard** – Specifies an ACL that filters packets based on the source IP address.

- **extended** – Specifies an ACL that filters packets based on the source or destination IP address, and other more specific criteria.
- *acl_name* – Name of the ACL. (Maximum length: 16 characters)

Default Setting

None

Command Mode

Global Configuration

Command Usage

- An ACL can contain either all permit commands or all deny commands.
- When you create a new ACL or enter configuration mode for an existing ACL, use the **permit** or **deny** command to add new rules to the bottom of the list. To create an ACL, you must add at least one rule to the list.
- To remove a rule, use the **no permit** or **no deny** command followed by the exact text of a previously configured rule.
- An ACL can contain up to 32 rules.

Example

```
Console(config)#access-list ip standard david
Console(config-std-acl)#
```

Related Commands

permit, deny 4-78
ip access-group (4-81)
show ip access-list (4-83)

permit, deny (Standard ACL)

Use this command to add a rule to a Standard IP ACL. The rule sets a filter condition for packets emanating from the specified source. Use the **no** form to remove a rule.

Syntax

{permit | deny} {any | *source bitmask* | host *source*}
no {permit | deny} {any | *source bitmask* | host *source*}

- **any** – Any source IP address.
- *source* – Source IP address.
- *bitmask* – Decimal number representing the address bits to match.
- **host** – Keyword followed by a specific IP address.

Default Setting

None

Command Mode

Standard ACL

Command Usage

- New rules are added to the end of the list.
- Address bitmasks are similar to a subnet mask, containing four integers from 0 to 255, each separated by a period. The binary mask uses 1 bits to indicate “match” and 0 bits to indicate “ignore.” The bitmask is bitwise ANDed with the specified source IP address, and then compared with the address for each IP packet entering the port(s) to which this ACL has been assigned.

Example

This example configures one permit rule for the specific address 10.1.1.21 and another rule for the address range 168.92.16.x – 168.92.31.x using a bitmask.

```
Console(config-std-acl)#permit host 10.1.1.21
Console(config-std-acl)#permit 168.92.16.0 255.255.240.0
Console(config-std-acl)#
```

Related Commands

access-list ip (4-76)

permit, deny (Extended ACL)

Use this command to add a rule to an Extended IP ACL. The rule sets a filter condition for packets with specific source and destination IP addresses, protocol types, source and destination TCP/UDP ports, or TCP control codes. Use the **no** form to remove a rule.

Syntax

```
{permit | deny} {any | source bitmask | host source}
    {any | destination bitmask | host destination} [protocol protocol-number]
no {permit | deny} {any | source bitmask | host source}
    {any | destination bitmask | host destination} [protocol protocol-number]

{permit | deny} {any | source bitmask | host source}
    {any | destination bitmask | host destination} {protocol tcp}
    [sport source-port] [dport destination-port]
    [control-code control-code code-bitmask]
no {permit | deny} {any | source bitmask | host source}
    {any | destination bitmask | host destination} {protocol tcp}
    [sport source-port] [dport destination-port]
    [control-code control-code code-bitmask]

{permit | deny} {any | source bitmask | host source}
    {any | destination bitmask | host destination} {protocol udp}
    [sport source-port] [dport destination-port]
no {permit | deny} {any | source bitmask | host source}
    {any | destination bitmask | host destination} {protocol udp}
    [sport source-port] [dport destination-port]
```

- **any** – Any IP address (source if first field, destination if second field).
- *source* – Source IP address.
- *destination* – Destination IP address.
- *bitmask* – Decimal number representing the address bits to match.

- **host** – Keyword followed by a specific IP address.
- *source-port* – TCP/UDP source port number. (Range: 0-65535)
- *destination-port* – TCP/UDP destination port number. (Range: 0-65535)
- *protocol-number* – A specific protocol number. (Range: 0-255)
- *control-code* – Decimal number (representing a bit string) that specifies flag bits in byte 14 of the TCP header. (Range: 0-63)
- *code-bitmask* – Decimal number representing the code bits to match.

Default Setting

None

Command Mode

Extended ACL

Command Usage

- All new rules are added to the end of the list.
- Address bitmasks are similar to a subnet mask, containing four integers from 0 to 255, each separated by a period. The binary mask uses 1 bits to indicate “match” and 0 bits to indicate “ignore.” The bitmask is bitwise ANDed with the specified source IP address, and then compared with the address for each IP packet entering the port(s) to which this ACL has been assigned.
- The control-code bitmask is a decimal number (representing an equivalent bit mask) that is applied to the control code. Enter a decimal number, where the equivalent binary bit “1” means to match a bit and “0” means to ignore a bit. The following bits may be specified:
 - 1 (fin) – Finish
 - 2 (syn) – Synchronize
 - 4 (rst) – Reset
 - 8 (psh) – Push
 - 16 (ack) – Acknowledgement
 - 32 (urg) – Urgent pointer

For example, use the code value and mask below to catch packets with the following flags set:

- SYN flag valid, use “control-code 2 2”

- Both SYN and ACK valid, use “control-code 18 18”
- SYN valid and ACK invalid, use “control-code 2 18”

Example

This example accepts any incoming packets if the source address is within subnet 10.7.1.x. For example, if the rule is matched; i.e., the rule (10.7.1.0 & 255.255.255.0) equals the masked address (10.7.1.2 & 255.255.255.0), the packet passes through.

```
Console(config-ext-acl)#permit 10.7.1.1 255.255.255.0 any
Console(config-ext-acl)#
```

This allows TCP packets from class C addresses 192.168.1.0 to any destination address when set for destination TCP port 80 (i.e., HTTP).

```
Console(config-ext-acl)#permit 192.168.1.0 255.255.255.0 any dport
80
Console(config-ext-acl)#
```

This permits all TCP packets from class C addresses 192.168.1.0 with the TCP control code set to “SYN.”

```
Console(config-ext-acl)#permit 192.168.1.0 255.255.255.0 any tcp
control-code 2 2
Console(config-ext-acl)#
```

Related Commands

access-list ip (4-76)

ip access-group

Use this command to bind a port to an IP ACL. Use the **no** form to remove the port.

Syntax

ip access-group *acl_name* **in**
no ip access-group *acl_name* **in**

- *acl_name* – Name of the ACL. (Maximum length: 16 characters)
- **in** – Indicates that this list applies to input packets.

Default Setting

None

Command Mode

Interface Configuration (Ethernet)

Example

```
Console(config)#int eth 1/25
Console(config-if)#ip access-group standard david in
Console(config-if)#
```

Related Commands

show ip access-list (4-83)

show ip access-group

Use this command to show the ports assigned to IP ACLs.

Command Mode

Privileged Exec

Example

```
Console#show ip access-group
Interface ethernet 1/25
  IP standard access-list david
Console#
```

Related Commands

ip access-group (4-81)

show ip access-list

Use this command to display the rules for configured IP ACLs.

Syntax

show ip access-list {standard | extended} [acl_name]

- **standard** – Specifies a standard IP ACL.
- **extended** – Specifies an extended IP ACL.
- *acl_name* – Name of the ACL. (Maximum length: 16 characters)

Command Mode

Privileged Exec

Example

```
Console#show ip access-list standard
IP standard access-list david:
  permit host 10.1.1.21
  permit 168.92.0.0 0.0.15.255
Console#
```

Related Commands

permit, deny (4-78, 4-79)
ip access-group (4-81)

MAC ACLs

Command	Function	Mode	Page
access-list mac	Creates a MAC ACL and enters configuration mode	GC	4-84
permit, deny	Filters packets matching a specified source and destination address, packet format, and Ethernet type	MAC-ACL	4-85
mac access-group	Adds a port to a MAC ACL	IC	4-87
show mac access-group	Shows port assignments for MAC ACLs	PE	4-87
show mac access-list	Displays the rules for configured MAC ACLs	PE	4-88

access-list mac

Use this command to add a MAC access list and enter MAC ACL configuration mode. Use the **no** form to remove the specified ACL.

Syntax

access-list mac *acl_name*

no access-list mac *acl_name*

acl_name – Name of the ACL. (Maximum length: 16 characters)

Default Setting

None

Command Mode

Global Configuration

Command Usage

- An ACL can contain either all permit commands or all deny commands.
- When you create a new ACL or enter configuration mode for an existing ACL, use the **permit** or **deny** command to add new rules to

the bottom of the list. To create an ACL, you must add at least one rule to the list.

- To remove a rule, use the **no permit** or **no deny** command followed by the exact text of a previously configured rule.
- An ACL can contain up to 32 rules.

Example

```
Console(config)#access-list mac jerry
Console(config-mac-acl)#
```

Related Commands

permit, deny (4-85)
 mac access-group (4-87)
 show mac access-list (4-88)

permit, deny (MAC ACL)

Use this command to add a rule to a MAC ACL. The rule filters packets matching a specified MAC source or destination address (i.e., physical layer address), or Ethernet protocol type. Use the **no** form to remove a rule.

Syntax

```
{permit | deny} [packet-format]
  {any | host source | source bitmask}
  {any | host destination | destination bitmask}
  {any | ethertype protocol}
```

```
no {permit | deny} [packet-format]
  {any | host source | source bitmask}
  {any | host destination | destination bitmask}
  {any | ethertype protocol}
```

- *packet-format* –
 - **tagged-802.3** – Tagged Ethernet 802.3 packets.
 - **tagged-eth2** – Tagged Ethernet II packets.
 - **untagged-802.3** – Untagged Ethernet 802.3 packets.
 - **untagged-eth2** – Untagged Ethernet II packets.

- **any** – Any MAC source address, destination address, or Ethernet protocol.
- *source* – Source MAC address.
- *source bitmask* – Binary mask for the source MAC address.
- *destination* – Destination MAC address.
- *destination bitmask* – Binary mask for the destination MAC address.
- *protocol* – A specific Ethernet protocol number. (Range: 0-65535)

Default Setting

None

Command Mode

MAC ACL

Command Usage

- New rules are added to the end of the list.
- The **ethertype** option can only be used to filter Ethernet II formatted packets.
- A detailed listing of Ethernet protocol types can be found in RFC 1060. A few of the more common types include the following:
 - 0800 - IP
 - 0806 - ARP
 - 8137 - IPX

Example

This rule permits packets from any source MAC address to the destination address 00-e0-29-94-34-de where the Ethernet type is 0800.

```
Console(config-mac-acl)#permit any host 00-e0-29-94-34-de  
ethertype 0800  
Console(config-mac-acl)#
```

Related Commands

access-list mac (4-84)

mac access-group

Use this command to bind a port to a MAC ACL. Use the **no** form to remove the port.

Syntax

mac access-group *acl_name* in

acl_name – Name of the ACL. (Maximum length: 16 characters)

Default Setting

None

Command Mode

Interface Configuration (Ethernet)

Command Usage

- A port can only be bound to one ACL.
- If a port is already bound to an ACL and you bind it to a different ACL, the switch will replace the old binding with the new one.

Example

```
Console(config)#interface ethernet 1/25
Console(config-if)#mac access-group jerry in
Console(config-if)#
```

Related Commands

show mac access-list (4-88)

show mac access-group

Use this command to show the ports assigned to MAC ACLs.

Command Mode

Privileged Exec

Example

```
Console#show mac access-group
Interface ethernet 1/25
MAC access-list jerry
Console#
```

Related Commands

mac access-group (4-87)

show mac access-list

Use this command to display the rules for configured MAC ACLs.

Syntax

show mac access-list [*acl_name*]

acl_name – Name of the ACL. (Maximum length: 16 characters)

Command Mode

Privileged Exec

Example

```
Console#show mac access-list
MAC access-list jerry:
  permit any 00-e0-29-94-34-de ethertype 0800
Console#
```

Related Commands

permit, deny 4-85

mac access-group (4-87)

ACL Information

Command	Function	Mode	Page
show access-list	Show all ACLs and associated rules	PE	4-89
show access-group	Shows the ACLs assigned to each port	PE	4-89

show access-list

Use this command to show all ACLs and associated rules.

Command Mode

Privileged Exec

Example

```

Console#show access-list
IP standard access-list david:
  permit host 10.1.1.21
  permit 168.92.0.0 0.0.15.255
IP extended access-list bob:
  permit 10.7.1.1 0.0.0.255 any
  permit 192.168.1.0 0.0.0.255 any dport 80
  permit 192.168.1.0 0.0.0.255 any protocol tcp control-code 2 2
MAC access-list jerry:
  permit any 00-30-29-94-34-de ethertype 800
Console#

```

show access-group

Use this command to show the port assignments of ACLs.

Command Mode

Privileged Executive

Example

```

Console#show access-group
Interface ethernet 1/25
  IP standard access-list david
  MAC access-list jerry
Console#

```

SNMP Commands

Controls access to this switch from management stations using the Simple Network Management Protocol (SNMP), as well as the error types sent to trap managers.

Command	Function	Mode	Page
snmp-server community	Sets up the community access string to permit access to SNMP commands	GC	4-90
snmp-server contact	Sets the system contact string	GC	4-91
snmp-server location	Sets the system location string	GC	4-92
snmp-server host	Specifies the recipient of an SNMP notification operation	GC	4-93
snmp-server enable traps	Enables the device to send SNMP traps (i.e., SNMP notifications)	GC	4-94
show snmp	Displays the status of SNMP communications	NE, PE	4-95

snmp-server community

Use this command to define the community access string for the Simple Network Management Protocol. Use the **no** form to remove the specified community string.

Syntax

snmp-server community *string* [**ro** | **rw**]

no snmp-server community *string*

- *string* - Community string that acts like a password and permits access to the SNMP protocol. (Maximum length: 32 characters, case sensitive; Maximum number of strings: 5)
- **ro** - Specifies read-only access. Authorized management stations are only able to retrieve MIB objects.
- **rw** - Specifies read/write access. Authorized management stations are able to both retrieve and modify MIB objects.

Default Setting

- public - Read-only access. Authorized management stations are only able to retrieve MIB objects.
- private - Read/write access. Authorized management stations are able to both retrieve and modify MIB objects.

Command Mode

Global Configuration

Command Usage

The first `snmp-server community` command you enter enables SNMP (SNMPv1). The `no snmp-server community` command disables SNMP.

Example

```
Console(config)#snmp-server community alpha rw
Console(config)#
```

snmp-server contact

Use this command to set the system contact string. Use the **no** form to remove the system contact information.

Syntax

snmp-server contact *string*

no snmp-server contact

string - String that describes the system contact information.
(Maximum length: 255 characters)

Default Setting

None

Command Mode

Global Configuration

Example

```
Console(config)#snmp-server contact Paul
Console(config)#
```

Related Commands

snmp-server location (4-92)

snmp-server location

Use this command to set the system location string. Use the **no** form to remove the location string.

Syntax

snmp-server location *text*

no snmp-server location

text - String that describes the system location.
(Maximum length: 255 characters)

Default Setting

None

Command Mode

Global Configuration

Example

```
Console(config)#snmp-server location WC-19
Console(config)#
```

Related Commands

snmp-server contact (4-91)

snmp-server host

Use this command to specify the recipient of a Simple Network Management Protocol notification operation. Use the **no** form to remove the specified host.

Syntax

snmp-server host *host-addr community-string*

no snmp-server host *host-addr*

- *host-addr* - Internet address of the host (the targeted recipient). (Maximum host addresses: 5 trap destination IP address entries)
- *community-string* - Password-like community string sent with the notification operation. Although you can set this string using the **snmp-server host** command by itself, we recommend that you define this string using the **snmp-server community** command prior to using the **snmp-server host** command. (Maximum length: 32 characters)

Default Setting

None

Command Mode

Global Configuration

Command Usage

- If you do not enter an **snmp-server host** command, no notifications are sent. In order to configure the switch to send SNMP notifications, you must enter at least one **snmp-server host** command. In order to enable multiple hosts, you must issue a separate **snmp-server host** command for each host.
- The **snmp-server host** command is used in conjunction with the **snmp-server enable traps** command. Use the **snmp-server enable traps** command to specify which SNMP notifications are sent globally. For a host to receive notifications, at least one **snmp-server enable traps** command and the **snmp-server host** command for that host must be enabled.

- However, some notification types cannot be controlled with the **snmp-server enable traps** command. For example, some notification types are always enabled.

Example

```
Console(config)#snmp-server host 10.1.19.23 batman
Console(config)#
```

Related Commands

snmp-server enable traps (4-94)

snmp-server enable traps

Use this command to enable this device to send Simple Network Management Protocol traps (SNMP notifications). Use the **no** form to disable SNMP notifications.

Syntax

snmp-server enable traps [authentication | link-up-down]
no snmp-server enable traps [authentication | link-up-down]

- **authentication** - Keyword to issue authentication failure traps.
- **link-up-down** - Keyword to issue link-up or link-down traps.
The link-up-down trap can only be enabled/disabled via the CLI.

Default Setting

Issue authentication and link-up-down traps.

Command Mode

Global Configuration

Command Usage

- If you do not enter an **snmp-server enable traps** command, no notifications controlled by this command are sent. In order to configure this device to send SNMP notifications, you must enter at least one **snmp-server enable traps** command. If you enter the command with no keywords, both authentication and link-up-down

notifications are enabled. If you enter the command with a keyword, only the notification type related to that keyword is enabled.

- The **snmp-server enable traps** command is used in conjunction with the **snmp-server host** command. Use the **snmp-server host** command to specify which host or hosts receive SNMP notifications. In order to send notifications, you must configure at least one **snmp-server host** command.

Example

```
Console(config)#snmp-server enable traps link-up-down
Console(config)#
```

Related Commands

snmp-server host (4-93)

show snmp

Use this command to check the status of SNMP communications.

Default Setting

None

Command Mode

Normal Exec, Privileged Exec

Command Usage

This command provides information on the community access strings, counter information for SNMP input and output protocol data units, and whether or not SNMP logging has been enabled with the **snmp-server enable traps** command.

Example

```
Console#show snmp

SNMP traps:
  Authentication: enable
  Link-up-down: enable

SNMP communities:
  1. private, and the privilege is read-write
  2. public, and the privilege is read-only

0 SNMP packets input
  0 Bad SNMP version errors
  0 Unknown community name
  0 Illegal operation for community name supplied
  0 Encoding errors
  0 Number of requested variables
  0 Number of altered variables
  0 Get-request PDUs
  0 Get-next PDUs
  0 Set-request PDUs

0 SNMP packets output
  0 Too big errors
  0 No such name errors
  0 Bad values errors
  0 General errors
  0 Response PDUs
  0 Trap PDUs

SNMP logging: disabled
Console#
```

DHCP Commands

These commands are used to configure Dynamic Host Configuration Protocol (DHCP) client, relay, and server functions. You can configure any VLAN interface to be automatically assigned an IP address via DHCP. This switch can be configured to relay DHCP client configuration requests to a DHCP server on another network, or you can configure this switch to provide DHCP service directly to any client.

Command Group	Function	Page
DHCP Client	Allows interfaces to dynamically acquire IP address information	4-97
DHCP Relay	Relays DHCP requests from local hosts to a remote DHCP server	4-99
DHCP Server	Configures DHCP service using address pools or static bindings	4-102

DHCP Client

Command	Function	Mode	Page
ip dhcp client-identifier	Specifies the DHCP client identifier for this switch	IC	4-97
ip dhcp restart client	Submits a BOOTP or DHCP client request	PE	4-98

ip dhcp client-identifier

Use this command to specify the DHCP client identifier for the current interface. Use the **no** form to remove this identifier.

Syntax

ip dhcp client-identifier {**text** *text* | **hex** *hex*}

no ip dhcp client-identifier

- *text* - A text string. (Range: 1-15 characters)
- *hex* - The hexadecimal value.

Default Setting

None

Command Mode

Interface Configuration (VLAN)

Command Usage

This command is used to include a client identifier in all communications with the DHCP server. The identifier type depends on the requirements of your DHCP server.

Example

```
Console(config)#interface vlan 2
Console(config-if)#ip dhcp client-identifier hex 00-00-e8-66-65-72
Console(config-if)#
```

Related Commands

ip dhcp restart client (4-98)

ip dhcp restart client

Use this command to submit a BOOTP or DHCP client request.

Default Setting

None

Command Mode

Privileged Exec

Command Usage

- This command issues a BOOTP or DHCP client request for any IP interface that has been set to BOOTP or DHCP mode via the **ip address** command.
- DHCP requires the server to reassign the client's last address if available.

- If the BOOTP or DHCP server has been moved to a different domain, the network portion of the address provided to the client will be based on this new domain.

Example

In the following example, the device is reassigned the same address.

```

Console(config)#interface vlan 1
Console(config-if)#ip address dhcp
Console(config-if)#exit
Console#ip dhcp restart client
Console#show ip interface

Vlan 1 is up, addressing mode is Dhcp
  Interface address is 10.1.0.254, mask is 255.255.255.0, Primary
  MTU is 1500 bytes
  Proxy ARP is disabled
  Split horizon is enabled
Console#

```

Related Commands

ip address (4-216)

DHCP Relay

Command	Function	Mode	Page
ip dhcp restart relay	Enables DHCP relay agent	IC	4-99
ip dhcp relay server	Specifies DHCP server addresses for relay	IC	4-101

ip dhcp restart relay

Use this command to enable DHCP relay for the specified VLAN. Use the **no** form to disable it.

Syntax

```

ip dhcp relay
no ip dhcp relay

```

Default Setting

Disabled

Command Mode

Interface Configuration (VLAN)

Command Usage

This command is used to configure DHCP relay functions for host devices attached to the switch. If DHCP relay service is enabled, and this switch sees a DHCP request broadcast, it inserts its own IP address into the request so the DHCP server will know the subnet where the client is located. Then, the switch forwards the packet to the DHCP server on another network. When the server receives the DHCP request, it allocates a free IP address for the DHCP client from its defined scope for the DHCP client's subnet, and sends a DHCP response back to the DHCP relay agent (i.e., this switch). This switch then broadcasts the DHCP response received from the server to the client.

Example

In the following example, the device is reassigned the same address.

```
Console(config)#interface vlan 1
Console(config-if)#ip dhcp relay
Console(config-if)#end
Console#show ip interface

Vlan 1 is up, addressing mode is Dhcp
  Interface address is 10.1.0.254, mask is 255.255.255.0, Primary
  MTU is 1500 bytes
  Proxy ARP is disabled
  Split horizon is enabled
Console#
```

Related Commands

ip dhcp relay server (4-101)

ip dhcp relay server

Use this command to specify the addresses of DHCP servers to be used by the switch's DHCP relay agent. Use the **no** form to clear all addresses.

Syntax

ip dhcp relay server *address1* [*address2* [*address3* ...]]

no ip dhcp relay server

address - IP address of DHCP server. (Range: 1-3 addresses)

Default Setting

None

Command Mode

Interface Configuration (VLAN)

Usage Guidelines

- You must specify the IP address for at least one DHCP server. Otherwise, the switch's DHCP relay agent will not forward client requests to a DHCP server.
- To start DHCP relay service, enter the **ip dhcp restart relay** command.

Example

```
Console(config)#interface vlan 1
Console(config-if)#ip dhcp relay server 10.1.0.99
Console(config-if)#
```

Related Commands

ip dhcp restart relay (4-99)

DHCP Server

Command	Function	Mode	Page
service dhcp	Enables the DHCP server feature on this switch	GC	4-103
ip dhcp excluded-address	Specifies IP addresses that a DHCP server should not assign to DHCP clients	GC	4-104
ip dhcp pool	Configures a DHCP address pool on a DHCP Server	GC	4-104
network	Configures the subnet number and mask for a DHCP address pool	DC	4-105
default-router	Specifies the default router list for a DHCP client	DC	4-106
domain-name	Specifies the domain name for a DHCP client	DC	4-107
dns-server	Specifies the Domain Name Server (DNS) servers available to a DHCP client	DC	4-108
next-server	Configures the next server in the boot process of a DHCP client	DC	4-109
bootfile	Specifies a default boot image for a DHCP client	DC	4-109
netbios-name-server	Configures NetBIOS Windows Internet Naming Service (WINS) name servers available to Microsoft DHCP clients	DC	4-110
netbios-node-type	Configures NetBIOS node type for Microsoft DHCP clients	DC	4-111
lease	Sets the duration an IP address is assigned to a DHCP client	DC	4-112
host*	Specifies the IP address and network mask to manually bind to a DHCP client	DC	4-113
client-identifier*	Specifies a client identifier for a DHCP client	DC	4-114
hardware-address*	Specifies the hardware address of a DHCP client	DC	4-115

Command	Function	Mode	Page
clear ip dhcp binding	Deletes an automatic address binding from the DHCP server database	PE	4-116
show ip dhcp binding	Displays address bindings on the DHCP server	PE, NE	4-117

* These commands are used for manually binding an address to a client.

service dhcp

Use this command to enable the DHCP server on this switch. Use the **no** form to disable the DHCP server.

Syntax

service dhcp
no service dhcp

Default Setting

Enabled

Command Mode

Global Configuration

Example

```
Console(config)#service dhcp
Console(config)#
```

ip dhcp excluded-address

Use this command to specify IP addresses that the DHCP server should not assign to DHCP clients. Use the **no** form to remove the excluded IP addresses.

Syntax

ip dhcp excluded-address *low-address* [*high-address*]
no ip dhcp excluded-address *low-address* [*high-address*]

- *low-address* - An excluded IP address, or the first IP address in an excluded address range.
- *high-address* - The last IP address in an excluded address range.

Default Setting

All IP pool addresses may be assigned.

Command Mode

Global Configuration

Example

```
Console(config)#ip dhcp excluded-address 10.1.0.19
Console(config)#
```

ip dhcp pool

Use this command to configure a DHCP address pool and enter DHCP Pool Configuration mode. Use the **no** form to remove the address pool.

Syntax

ip dhcp pool *name*
no ip dhcp pool *name*

name - A string or integer. (Range: 1-8 characters)

Default Setting

DHCP address pools are not configured.

Command Mode

Global Configuration

Usage Guidelines

- After executing this command, the switch changes to DHCP Pool Configuration mode, identified by the (config-dhcp)# prompt.
- From this mode, first configure address pools for the network interfaces (using the **network** command). You can also manually bind an address to a specific client (with the **host** command) if required. You can configure up to 8 network address pools, and up to 32 manually bound host address pools (i.e., listing one host address per pool). However, note that any address specified in a **host** command must fall within the range of a configured network address pool.

Example

```
Console(config)#ip dhcp pool R&D
Console(config-dhcp)#
```

Related Commands

network (4-105)

host (4-113)

network

Use this command to configure the subnet number and mask for a DHCP address pool. Use the **no** form to remove the subnet number and mask.

Syntax

network *network-number* [*mask*]

no network

- *network-number* - The IP address of the DHCP address pool.
- *mask* - The bit combination that identifies the network (or subnet) and the host portion of the DHCP address pool.

Command Mode

DHCP Pool Configuration

Usage Guidelines

- When a client request is received, the switch first checks for a network address pool matching the gateway where the request originated (i.e., if the request was forwarded by a relay server). If there is no gateway in the client request (i.e., the request was not forwarded by a relay server), the switch searches for a network pool matching the interface through which the client request was received. It then searches for a manually configured host address that falls within the matching network pool. If no manually configured host address is found, it assigns an address from the matching network address pool. However, if no matching address pool is found the request is ignored.
- This command is valid for DHCP network address pools only. If the mask is not specified, the class A, B, or C natural mask is used (see page 3-178). The DHCP server assumes that all host addresses are available. You can exclude subsets of the address space by using the **dhcp excluded-address** command.

Example

```
Console(config-dhcp)#network 10.1.0.0 255.255.255.0
Console(config-dhcp)#
```

default-router

Use this command to specify default routers for a DHCP pool. Use the **no** form to remove the default routers.

Syntax

default-router *address1* [*address2*]

no default-router

- *address1* - Specifies the IP address of the primary router.
- *address2* - Specifies the IP address of an alternate router.

Default Setting

None

Command Mode

DHCP Pool Configuration

Usage Guidelines

The IP address of the router should be on the same subnet as the client. You can specify up to two routers. Routers are listed in order of preference (starting with *address1* as the most preferred router).

Example

```
Console(config-dhcp)#default-router 10.1.0.54 10.1.0.64
Console(config-dhcp)#
```

domain-name

Use this command to specify the domain name for a DHCP client. Use the **no** form to remove the domain name.

Syntax

domain-name *domain*

no domain-name

domain - Specifies the domain name of the client.
(Range: 1-32 characters)

Default Setting

None

Command Mode

DHCP Pool Configuration

Example

```
Console(config-dhcp)#domain-name sample.com
Console(config-dhcp)#
```

dns-server

Use this command to specify the Domain Name System (DNS) IP servers available to a DHCP client. Use the **no** form to remove the DNS server list.

Syntax

dns-server *address1* [*address2*]

no dns-server

- *address1* - Specifies the IP address of the primary DNS server.
- *address2* - Specifies the IP address of the alternate DNS server.

Default Setting

None

Command Mode

DHCP Pool Configuration

Usage Guidelines

- If DNS IP servers are not configured for a DHCP client, the client cannot correlate host names to IP addresses.
- Servers are listed in order of preference (starting with *address1* as the most preferred server).

Example

```
Console(config-dhcp)#dns-server 10.1.1.253 192.168.3.19
Console(config-dhcp)#
```

next-server

Use this command to configure the next server in the boot process of a DHCP client. Use the **no** form to remove the boot server list.

Syntax

next-server *address*

no next-server *address*

address - Specifies the IP address of the next server in the boot process, which is typically a Trivial File Transfer Protocol (TFTP) server.

Default Setting

None

Command Mode

DHCP Pool Configuration

Example

```
Console(config-dhcp)#next-server 10.1.0.21
Console(config-dhcp)#
```

Related Commands

bootfile (4-109)

bootfile

Use this command to specify the name of the default boot image for a DHCP client. This file should be placed on the Trivial File Transfer Protocol (TFTP) server specified with the **next-server** command. Use the **no** form to delete the boot image name.

Syntax

bootfile *filename*

no bootfile

filename - Name of the file that is used as a default boot image.

Default Setting

None

Command Mode

DHCP Pool Configuration

Example

```
Console(config-dhcp)#bootfile wme.bat
Console(config-dhcp)#
```

Related Commands

next-server (4-109)

netbios-name-server

Use this command to configure NetBIOS Windows Internet Naming Service (WINS) name servers that are available to Microsoft DHCP clients. Use the **no** form to remove the NetBIOS name server list.

Syntax

netbios-name-server *address1* [*address2*]

no netbios-name-server

- *address1* - Specifies IP address of primary NetBIOS WINS name server.
- *address2* - Specifies IP address of alternate NetBIOS WINS name server.

Default Setting

None

Command Mode

DHCP Pool Configuration

Usage Guidelines

Servers are listed in order of preference (starting with *address1* as the most preferred server).

Example

```
Console(config-dhcp)#netbios-name-server 10.1.0.33 10.1.0.34
Console(config-dhcp)#
```

Related Commands

netbios-node-type (4-111)

netbios-node-type

Use this command to configure the NetBIOS node type for Microsoft DHCP clients. Use the **no** form to remove the NetBIOS node type.

Syntax

netbios-node-type *type*

no netbios-node-type

type - Specifies the NetBIOS node type:

- **broadcast**
- **hybrid** (recommended)
- **mixed**
- **peer-to-peer**

Default Setting

None

Command Mode

DHCP Pool Configuration

Example

```
Console(config-dhcp)#netbios-node-type hybrid
Console(config-dhcp)#
```

Related Commands

netbios-name-server (4-110)

lease

Use this command to configure the duration that an IP address is assigned to a DHCP client. Use the **no** form to restore the default value.

Syntax

lease {*days* [*hours*][*minutes*] | **infinite**}

no lease

- *days* - Specifies the duration of the lease in numbers of days. (Range: 0-364)
- *hours* - Specifies the number of hours in the lease. A *days* value must be supplied before you can configure *hours*. (Range: 0-23)
- *minutes* - Specifies the number of minutes in the lease. A *days* and *hours* value must be supplied before you can configure *minutes*. (Range: 0-59)
- **infinite** - Specifies that the lease time is unlimited. This option is normally used for addresses manually bound to a BOOTP client via the **host** command.

Default Setting

One day

Command Modes

DHCP Pool Configuration

Example

The following example leases an address to clients using this pool for 7 days.

```
Console(config-dhcp)#lease 7
Console(config-dhcp)#
```

host

Use this command to specify the IP address and network mask to manually bind to a DHCP client. Use the **no** form to remove the IP address for the client.

Syntax

host *address* [*mask*]

no host

- *address* - Specifies the IP address of a client.
- *mask* - Specifies the network mask of the client.

Default Setting

None

Command Mode

DHCP Pool Configuration

Usage Guidelines

- Host addresses must fall within the range specified for an existing network pool.
- When a client request is received, the switch first checks for a network address pool matching the gateway where the request originated (i.e., if the request was forwarded by a relay server). If there is no gateway in the client request (i.e., the request was not forwarded by a relay server), the switch searches for a network pool matching the interface through which the client request was received. It then searches for a manually configured host address that falls within the matching network pool.
- When searching for a manual binding, the switch compares the client identifier for DHCP clients, and then compares the hardware address for DHCP or BOOTP clients.
- If no manual binding has been specified for a host entry with the **client-identifier** or **hardware-address** commands, then the switch will assign an address from the matching network pool.
- If the mask is unspecified, DHCP examines its address pools. If no mask is found in the pool database, the Class A, B, or C natural mask

is used (see page 3-178). This command is valid for manual bindings only.

- The **no host** command only clears the address from the DHCP server database. It does not cancel the IP address currently in use by the host.

Example

```
Console(config-dhcp)#host 10.1.0.21 255.255.255.0
Console(config-dhcp)#
```

Related Commands

client-identifier (4-114)
hardware-address (4-115)

client-identifier

Use this command to specify the client identifier of a DHCP client. Use the **no** form to remove the client identifier.

Syntax

client-identifier {text *text* | hex *hex*}
no client-identifier

- *text* - A text string. (Range: 1-15 characters)
- *hex* - The hexadecimal value.

Default Setting

None

Command Mode

DHCP Pool Configuration

Command Usage

- This command identifies a DHCP client to bind to an address specified in the **host** command. If both a client identifier and hardware address are configured for a host address, the client identifier takes precedence over the hardware address in the search procedure.

- BOOTP clients cannot transmit a client identifier. To bind an address to a BOOTP client, you must associate a hardware address with the host entry.

Example

```
Console(config-dhcp)#client-identifier text steve
Console(config-dhcp)#
```

Related Commands

host (4-113)

hardware-address

Use this command to specify the hardware address of a DHCP client. This command is valid for manual bindings only. Use the **no** form to remove the hardware address.

Syntax

hardware-address *hardware-address type*

no hardware-address

- *hardware-address* - Specifies the MAC address of the client device.
- *type* - Indicates the following protocol used on the client device:
 - **ethernet**
 - **ieee802**
 - **fddi**

Default Setting

If no type is specified, the default protocol is Ethernet.

Command Mode

DHCP Pool Configuration

Command Usage

This command identifies a DHCP or BOOTP client to bind to an address specified in the host command. BOOTP clients cannot transmit a client identifier. To bind an address to a BOOTP client, you must associate a hardware address with the host entry.

Example.

```
Console(config-dhcp)#hardware-address 00-e0-29-94-34-28 ethernet
Console(config-dhcp)#
```

Related Commands

host (4-113)

clear ip dhcp binding

Use this command to delete an automatic address binding from the DHCP server database.

Syntax

clear ip dhcp binding {*address* | *}

- *address* - The address of the binding to clear.
- * - Clears all automatic bindings.

Default Setting

None

Command Mode

Privileged Exec

Usage Guidelines

- An *address* specifies the client's IP address. If an asterisk (*) is used as the address parameter, the DHCP server clears all automatic bindings.
- Use the **no host** command to delete a manual binding.
- This command is normally used after modifying the address pool, or after moving DHCP service to another device.

Example

```
Console#clear ip dhcp binding *
Console#
```

Related Commands

show ip dhcp binding (4-117)

show ip dhcp binding

Use this command to display address bindings on the DHCP server.

Syntax

show ip dhcp binding [*address*]

address - Specifies the IP address of the DHCP client for which bindings will be displayed.

Default Setting

None

Command Mode

Normal Exec, Privileged Exec

Example

```
Console#show ip dhcp binding

      IP                MAC                Lease Time      Start
-----
192.1.3.21  00-00-e8-98-73-21      86400 Dec 25 08:01:57 2002
Console#
```

Interface Commands

These commands are used to display or set communication parameters for an Ethernet port, aggregated link, or VLAN.

Command	Function	Mode	Page
interface	Configures an interface type and enters interface configuration mode	GC	4-119
description	Adds a description to an interface configuration	IC	4-119
speed-duplex	Configures the speed and duplex operation of a given interface when autonegotiation is disabled	IC	4-120
negotiation	Enables autonegotiation of a given interface	IC	4-121
capabilities	Advertises the capabilities of a given interface for use in autonegotiation	IC	4-122
flowcontrol	Enables flow control on a given interface	IC	4-124
shutdown	Disables an interface	IC	4-125
switchport broadcast packet-rate	Configures the broadcast storm control threshold	IC	4-126
clear counters	Clears statistics on an interface	PE	4-127
show interfaces status	Displays status for the specified interface	NE, PE	4-128
show interfaces counters	Displays statistics for the specified interfaces	NE, PE	4-129
show interfaces switchport	Displays the administrative and operational status of an interface	NE, PE	4-131

interface

Use this command to configure an interface type and enter interface configuration mode. Use the **no** form to remove a trunk.

Syntax

interface *interface*

no interface port-channel *channel-id*

interface

- **ethernet** *unit/port*
 - *unit* - This is device 1.
 - *port* - Port number.
- **port-channel** *channel-id* (Range: 1-6)
- **vlan** *vlan-id* (Range: 1-4094)

Default Setting

None

Command Mode

Global Configuration

Example

To specify port 25, enter the following command:

```
Console(config)#interface ethernet 1/25
Console(config-if)#
```

description

Use this command to add a description to an interface. Use the **no** form to remove the description.

Syntax

description *string*

no description

string - Comment or a description to help you remember what is attached to this interface. (Range: 1-64 characters)

Default Setting

None

Command Mode

Interface Configuration (Ethernet, Port Channel)

Example

The following example adds a description to port 25.

```
Console(config)#interface ethernet 1/25
Console(config-if)#description RD-SW#3
Console(config-if)#
```

speed-duplex

Use this command to configure the speed and duplex mode of a given interface when autonegotiation is disabled. Use the **no** form to restore the default.

Syntax

speed-duplex {1000full | 100full | 100half | 10full | 10half}
no speed-duplex

- **1000full** - Forces 1000 Mbps full-duplex operation
- **100full** - Forces 100 Mbps full-duplex operation
- **100half** - Forces 100 Mbps half-duplex operation
- **10full** - Forces 10 Mbps full-duplex operation
- **10half** - Forces 10 Mbps half-duplex operation

Default Setting

- Auto-negotiation is enabled by default.
- When auto-negotiation is disabled, the default speed-duplex setting is 100half for 100BASE-TX ports and 1000full for Gigabit Ethernet ports.

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- To force operation to the speed and duplex mode specified in a **speed-duplex** command, use the **no negotiation** command to disable auto-negotiation on the selected interface.
- When using the **negotiation** command to enable auto-negotiation, the optimal settings will be determined by the **capabilities** command. To set the speed/duplex mode under auto-negotiation, the required mode must be specified in the capabilities list for an interface.

Example

The following example configures port 5 to 100 Mbps, half-duplex operation.

```
Console(config)#interface ethernet 1/5
Console(config-if)#speed-duplex 100half
Console(config-if)#no negotiation
Console(config-if)#
```

Related Commands

negotiation (4-121)

capabilities (4-122)

negotiation

Use this command to enable autonegotiation for a given interface. Use the **no** form to disable autonegotiation.

Syntax

negotiation

no negotiation

Default Setting

Enabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- When auto-negotiation is enabled the switch will negotiate the best settings for a link based on the **capabilities** command. When auto-negotiation is disabled, you must manually specify the link attributes with the **speed-duplex** and **flowcontrol** commands.
- If autonegotiation is disabled, auto-MDI/MDI-X pin signal configuration will also be disabled for the RJ-45 ports.

Example

The following example configures port 11 to use autonegotiation.

```
Console(config)#interface ethernet 1/11
Console(config-if)#negotiation
Console(config-if)#
```

Related Commands

capabilities (4-122)
speed-duplex (4-120)

capabilities

Use this command to advertise the port capabilities of a given interface during autonegotiation. Use the **no** form with parameters to remove an advertised capability, or the **no** form without parameters to restore the default values.

Syntax

capabilities {**1000full** | **100full** | **100half** | **10full** | **10half** | **flowcontrol** | **symmetric**}
no capabilities [**1000full** | **100full** | **100half** | **10full** | **10half** | **flowcontrol** | **symmetric**]

- **1000full** - Supports 1000 Mbps full-duplex operation
- **100full** - Supports 100 Mbps full-duplex operation
- **100half** - Supports 100 Mbps half-duplex operation
- **10full** - Supports 10 Mbps full-duplex operation
- **10half** - Supports 10 Mbps half-duplex operation
- **flowcontrol** - Supports flow control

- **symmetric** (Gigabit only) - When specified, the port transmits and receives pause frames; when not specified, the port will auto-negotiate to determine the sender and receiver for asymmetric pause frames. (*The current switch ASIC only supports symmetric pause frames.*)

Default Setting

- 100BASE-TX: 10half, 10full, 100half, 100full
- 1000BASE-T: 10half, 10full, 100half, 100full, 1000full
- 1000BASE-SX/LX/LH: 1000full

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

When auto-negotiation is enabled with the **negotiation** command, the switch will negotiate the best settings for a link based on the **capabilities** command. When auto-negotiation is disabled, you must manually specify the link attributes with the **speed-duplex** and **flowcontrol** commands.

Example

The following example configures Ethernet port 5 capabilities to 100half, 100full and flow control.

```
Console(config)#interface ethernet 1/5
Console(config-if)#capabilities 100half
Console(config-if)#capabilities 100full
Console(config-if)#capabilities flowcontrol
Console(config-if)#
```

Related Commands

negotiation (4-121)
speed-duplex (4-120)
flowcontrol (4-124)

flowcontrol

Use this command to enable flow control. Use the **no** form to disable flow control.

Syntax

flowcontrol
no flowcontrol

Default Setting

Flow control enabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- Flow control can eliminate frame loss by “blocking” traffic from end stations or segments connected directly to the switch when its buffers fill. When enabled, back pressure is used for half-duplex operation and IEEE 802.3x for full-duplex operation.
- To force flow control on or off (with the **flowcontrol** or **no flowcontrol** command), use the **no negotiation** command to disable auto-negotiation on the selected interface.
- When using the **negotiation** command to enable auto-negotiation, the optimal settings will be determined by the **capabilities** command. To enable flow control under auto-negotiation, “flowcontrol” must be included in the capabilities list for any port
- Avoid using flow control on a port connected to a hub unless it is actually required to solve a problem. Otherwise back pressure jamming signals may degrade overall performance for the segment attached to the hub.

Example

The following example enables flow control on port 5.

```
Console(config)#interface ethernet 1/5
Console(config-if)#flowcontrol
Console(config-if)#no negotiation
Console(config-if)#
```

Related Commands

negotiation (4-121)

capabilities (flowcontrol, symmetric) (4-122)

shutdown

Use this command to disable an interface. To restart a disabled interface, use the **no** form.

Syntax

shutdown

no shutdown

Default Setting

All interfaces are enabled.

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

This command allows you to disable a port due to abnormal behavior (e.g., excessive collisions), and then reenable it after the problem has been resolved. You may also want to disable a port for security reasons.

Example

The following example disables port 5.

```
Console(config)#interface ethernet 1/5
Console(config-if)#shutdown
Console(config-if)#
```

switchport broadcast packet-rate

Use this command to configure broadcast storm control. Use the **no** form to disable broadcast storm control.

Syntax

switchport broadcast packet-rate *rate*

no switchport broadcast

rate - Threshold level as a rate; i.e., packets per second.

(Range: 500 - 262143)

Default Setting

Enabled for all ports

Packet-rate limit: 500 packets per second

Command Mode

Interface Configuration (Ethernet)

Command Usage

- When broadcast traffic exceeds the specified threshold, packets above that threshold are dropped.
- This command can enable or disable broadcast storm control for the selected interface. However, the specified threshold value applies to all ports on the switch.

Example

The following shows how to configure broadcast storm control at 600 packets per second:

```
Console(config)#interface ethernet 1/5
Console(config-if)#switchport broadcast packet-rate 600
Console(config-if)#
```

clear counters

Use this command to clear statistics on an interface.

Syntax

clear counters *interface*

interface

- **ethernet** *unit/port*
 - *unit* - This is device 1.
 - *port* - Port number.
- **port-channel** *channel-id* (Range: 1-6)

Default Setting

None

Command Mode

Privileged Exec

Command Usage

Statistics are only initialized for a power reset. This command sets the base value for displayed statistics to zero for the current management session. However, if you log out and back into the management interface, the statistics displayed will show the absolute value accumulated since the last power reset.

Example

The following example clears statistics on port 5.

```
Console#clear counters ethernet 1/5
Console#
```

show interfaces status

Use this command to display the status for an interface.

Syntax

show interfaces status [*interface*]

interface

- **ethernet** *unit/port*
 - *unit* - This is device 1.
 - *port* - Port number.
- **port-channel** *channel-id* (Range: 1-6)
- **vlan** *vlan-id* (Range: 1-4094)

Default Setting

Shows the status for all interfaces.

Command Mode

Normal Exec, Privileged Exec

Command Usage

If no interface is specified, information on all interfaces is displayed.

For a description of the items displayed by this command, see

“Displaying Connection Status” on page 3-63.

Example

```

Console#show interfaces status ethernet 1/5
Information of Eth 1/5
Basic information:
  Port type: 100TX
  Mac address: 00-00-AB-CD-00-01
Configuration:
  Name:
  Port admin: Up
  Speed-duplex: Auto
  Capabilities: 10half, 10full, 100half, 100full,
  Broadcast storm: Enabled
  Broadcast storm limit: 500 packets/second
  Flow control: Disabled
  LACP: Disabled
Current status:
  Link status: Up
  Port operation status: Up
  Operation speed-duplex: 100full
  Flow control type: None
Console#show interfaces status vlan 1
Information of VLAN 1
MAC address: 00-00-AB-CD-00-00
Console#

```

show interfaces counters

Use this command to display interface statistics.

Syntax

show interfaces counters [*interface*]

interface

- **ethernet** *unit/port*
 - *unit* - This is device 1.
 - *port* - Port number.
- **port-channel** *channel-id* (Range: 1-6)

Default Setting

Shows the counters for all interfaces.

Command Mode

Normal Exec, Privileged Exec

Command Usage

If no interface is specified, information on all interfaces is displayed.
For a description of the items displayed by this command, see
“Showing Port Statistics” on page 3-71.

Example

```
Console#show interfaces counters ethernet 1/7
Ethernet 1/7
Iftable stats:
Octets input: 30658, Octets output: 196550
Unicast input: 6, Unicast output: 5
Discard input: 0, Discard output: 0
Error input: 0, Error output: 0
Unknown protos input: 0, QLen output: 0
Extended iftable stats:
Multi-cast input: 0, Multi-cast output: 3064
Broadcast input: 262, Broadcast output: 1
Ether-like stats:
Alignment errors: 0, FCS errors: 0
Single Collision frames: 0, Multiple collision frames: 0
SQE Test errors: 0, Deferred transmissions: 0
Late collisions: 0, Excessive collisions: 0
Internal mac transmit errors: 0, Internal mac receive errors: 0
Frame too longs: 0, Carrier sense errors: 0
Symbol errors: 0
RMON stats:
Drop events: 0, Octets: 227208, Packets: 3338
Broadcast pkts: 263, Multi-cast pkts: 3064
Undersize pkts: 0, Oversize pkts: 0
Fragments: 0, Jabbers: 0
CRC align errors: 0, Collisions: 0
Packet size <= 64 octets: 3150, Packet size 65 to 127 octets: 139
Packet size 128 to 255 octets: 49, Packet size 256 to 511 octets: 0
Packet size 512 to 1023 octets: 0, Packet size 1024 to 1518 octets: 0
Console#
```


show interfaces switchport

Use this command to display the administrative and operational status of the specified interfaces.

Syntax

show interfaces switchport [*interface*]

interface

- **ethernet** *unit/port*
 - *unit* - This is device 1.
 - *port* - Port number.
- **port-channel** *channel-id* (Range: 1-6)

Default Setting

Shows all interfaces.

Command Mode

Normal Exec, Privileged Exec

Command Usage

If no interface is specified, information on all interfaces is displayed.

Example

This example shows the configuration setting for port 25.

```
Console#show interfaces switchport ethernet 1/25
Broadcast threshold: Enabled, 500 packets/second
Lacp status: Disabled
VLAN membership mode: Hybrid
Ingress rule: Disabled
Acceptable frame type: All frames
Native VLAN: 1
Priority for untagged traffic: 0
Gvrp status: Disabled
Allowed Vlan: 1(u),
Forbidden Vlan:
Console#
```

Field	Description
Broadcast threshold	Shows if broadcast storm suppression is enabled or disabled; if enabled it also shows the threshold level (page 4-126).
Lacp status	Shows if Link Aggregation Control Protocol has been enabled or disabled (page 4-139).
VLAN membership mode	Indicates membership mode as Trunk or Hybrid (page 4-166).
Ingress rule	Shows if ingress filtering is enabled or disabled (page 4-168).
Acceptable frame type	Shows if acceptable VLAN frames include all types or tagged frames only (page 4-167).
Native VLAN	Indicates the default Port VLAN ID (page 4-169).
Priority for untagged traffic	Indicates the default priority for untagged frames (page 4-181).
Gvrp status	Shows if GARP VLAN Registration Protocol is enabled or disabled (page 4-177).
Allowed Vlan	Shows the VLANs this interface has joined, where “(u)” indicates untagged and “(t)” indicates tagged (page 4-170).
Forbidden Vlan	Shows the VLANs this interface can not dynamically join via GVRP (page 4-171).

Mirror Port Commands

This section describes how to mirror traffic from a source port to a target port.

Command	Function	Mode	Page
port monitor	Configures a mirror session	IC	4-133
show port monitor	Shows the configuration for a mirror port	PE	4-134

port monitor

Use this command to configure a mirror session. Use the **no** form to clear a mirror session.

Syntax

port monitor *interface* [**rx** | **tx** | **both**]

no port monitor *interface*

- *interface* - **ethernet** *unit/port* (source port)
 - *unit* - Switch (unit 1).
 - *port* - Port number.
- **rx** - Mirror received packets.
- **tx** - Mirror transmitted packets.
- **both** - Mirror both received and transmitted packets.

Default Setting

No mirror session is defined. When enabled, the default mirroring is for both received and transmitted packets.

Command Mode

Interface Configuration (Ethernet, destination port)

Command Usage

- You can mirror traffic from any source port to a destination port for real-time analysis. You can then attach a logic analyzer or RMON

probe to the destination port and study the traffic crossing the source port in a completely unobtrusive manner.

- The destination port is set by specifying an Ethernet interface.
- The mirror port and monitor port speeds should match, otherwise traffic may be dropped from the monitor port.
- You can create multiple mirror sessions, but all sessions must share the same destination port. However, you should avoid sending too much traffic to the destination port from multiple source ports.

Example

The following example configures the switch to mirror all packets from port 6 to port 11:

```
Console(config)#interface ethernet 1/11
Console(config-if)#port monitor ethernet 1/6 both
Console(config-if)#
```

show port monitor

Use this command to display mirror information.

Syntax

show port monitor [*interface*]

interface - **ethernet** *unit/port* (source port)

- *unit* - Switch (unit 1).
- *port* - Port number.

Default Setting

Shows all sessions.

Command Mode

Privileged Exec

Command Usage

This command displays the currently configured source port, destination port, and mirror mode (i.e., RX, TX, RX/TX).

Example

The following shows mirroring configured from port 6 to port 11:

```

Console(config)#interface ethernet 1/11
Console(config-if)#port monitor ethernet 1/6
Console(config-if)#end
Console#show port monitor
Port Mirroring
-----
Destination port(listen port):Eth1/1
Source port(monitored port)  :Eth1/6
Mode                        :RX/TX
Console#

```

Rate Limit Commands

This function allows the network manager to control the maximum rate for traffic transmitted or received on an interface. Rate limiting is configured on interfaces at the edge of a network to limit traffic into or out of the network. Traffic that falls within the rate limit is transmitted, while packets that exceed the acceptable amount of traffic are dropped.

Rate limiting can be applied to individual ports or trunks. When an interface is configured with this feature, the traffic rate will be monitored by the hardware to verify conformity. Non-conforming traffic is dropped, conforming traffic is forwarded without any changes.

Command	Function	Mode	Page
rate-limit	Configures the maximum input or output rate for a port	IC	4-136

rate-limit

Use this command to define the rate limit for a specific interface. Use this command without specifying a rate to restore the default rate. Use the **no** form to restore the default status of disabled.

Syntax

rate-limit {input | output} [*rate*]

no rate-limit {input | output}

- **input** – Input rate
- **output** – Output rate
- *rate* – Maximum value in Mbps.

Default Setting

Fast Ethernet interface – 100 Mbps

Gigabit Ethernet interface – 1000 Mbps

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- The range is:
 - Fast Ethernet interface – 1 to 100 Mbps
 - Gigabit Ethernet interface – 8 to 1000 Mbps
- Resolution – The increment of change:
 - Fast Ethernet interface – 1 Mbps
 - Gigabit Ethernet interface – 8 Mbps
- Due to a switch chip limitation, the input rate limit can only be enabled or disabled for all interfaces. In other words, the **rate limit input** and **no rate limit input** commands apply globally to the entire switch. However, specific rates apply to the specified interface.
- The output rate limit can be enabled or disabled for specific interfaces.

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#rate-limit input 10
Console(config-if)#
```

Link Aggregation Commands

Ports can be statically grouped into an aggregate link (i.e., trunk) to increase the bandwidth of a network connection or to ensure fault recovery. Or you can use the Link Aggregation Control Protocol (LACP) to automatically negotiate a trunk link between this switch and another network device. For static trunks, the switches have to comply with the Cisco EtherChannel standard. For dynamic trunks, the switches have to comply with LACP. This switch supports up to six trunks. For example, a trunk consisting of two 1000 Mbps ports can support an aggregate bandwidth of 4 Gbps when operating at full duplex.

Command	Function	Mode	Page
<i>Manual Configuration Commands</i>			
interface port-channel	Configures a trunk and enters interface configuration mode for the trunk	GC	4-119
channel-group	Adds a port to a trunk	IC	4-138
<i>Dynamic Configuration Command</i>			
lacp	Configures LACP for the current interface	IC	4-139
<i>Trunk Status Display Command</i>			
show interfaces status port-channel	Shows trunk information	NE, PE	4-128

Guidelines for Creating Trunks

- Finish configuring port trunks before you connect the corresponding network cables between switches to avoid creating a loop.
- A trunk can have up to four 10/100 Mbps ports or up to two 1000 Mbps ports.
- The ports at both ends of a connection must be configured as trunk ports.
- All ports in a trunk must consist of the same media type (i.e., twisted-pair or fiber).
- All ports in a trunk must be configured in an identical manner, including communication mode (i.e., speed, duplex mode and flow control), VLAN assignments, and CoS settings.

- All the ports in a trunk have to be treated as a whole when moved from/to, added or deleted from a VLAN via the specified port-channel.
- STP, VLAN, and IGMP settings can only be made for the entire trunk via the specified port-channel.

channel-group

Use this command to add a port to a trunk. Use the **no** form to remove a port from a trunk.

Syntax

channel-group *channel-id*
no channel-group
channel-id - Trunk index (Range: 1-6)

Default Setting

The current port will be added to this trunk.

Command Mode

Interface Configuration (Ethernet)

Command Usage

- When configuring static trunks, the switches must comply with the Cisco EtherChannel standard.
- Use **no channel-group** to remove a port group from a trunk.
- Use **no interfaces port-channel** to remove a trunk from the switch.

Example

The following example creates trunk 1 and then adds port 11:

```
Console(config)#interface port-channel 1
Console(config-if)#exit
Console(config)#interface ethernet 1/11
Console(config-if)#channel-group 1
Console(config-if)#
```


lacp

Use this command to enable 802.3ad Link Aggregation Control Protocol (LACP) for the current interface. Use the **no** form to disable it.

Syntax

lacp
no lacp

Default Setting

Disabled

Command Mode

Interface Configuration (Ethernet)

Command Usage

- The ports on both ends of an LACP trunk must be configured for full duplex, either by forced mode or auto-negotiation.
- A trunk formed with another switch using LACP will automatically be assigned the next available port-channel ID.
- If the target switch has also enabled LACP on the connected ports, the trunk will be activated automatically.
- If more than four ports attached to the same target switch have LACP enabled, the additional ports will be placed in standby mode, and will only be enabled if one of the active links fails.

Example

The following shows LACP enabled on ports 11-13. Because LACP has also been enabled on the ports at the other end of the links, the **show interfaces status port-channel 1** command shows that Trunk1 has been established.

```
Console(config)#interface ethernet 1/11
Console(config-if)#lACP
Console(config-if)#exit
Console(config)#interface ethernet 1/12
Console(config-if)#lACP
Console(config-if)#exit
Console(config)#interface ethernet 1/13
Console(config-if)#lACP
Console(config-if)#exit
Console(config)#exit
Console#show interfaces status port-channel 1
Information of Trunk 1
Basic information:
  Port type: 100tx
  Mac address: 00-00-e8-00-00-0b
Configuration:
  Name:
  Port admin status: Up
  Speed-duplex: Auto
  Capabilities: 10half, 10full, 100half, 100full,
  Flow control status: Disabled
Current status:
  Created by: lACP
  Link status: Up
  Operation speed-duplex: 100full
  Flow control type: None
  Member Ports: Eth1/11, Eth1/12, Eth1/13,
Console#
```

Address Table Commands

These commands are used to configure the address table for filtering specified addresses, displaying current entries, clearing the table, or setting the aging time.

Command	Function	Mode	Page
mac-address-table static	Maps a static address to a port in a VLAN	GC	4-141
clear mac-address-table dynamic	Removes any learned entries from the forwarding database	PE	4-142
show mac-address-table	Displays entries in the bridge-forwarding database	PE	4-143
mac-address-table aging-time	Sets the aging time of the address table	GC	4-144
show mac-address-table aging-time	Shows the aging time for the address table	PE	4-145

mac-address-table static

Use this command to map a static address to a destination port in a VLAN. Use the **no** form to remove an address.

Syntax

mac-address-table static *mac-address* **interface** *interface*
vlan *vlan-id* [*action*]

no mac-address-table static *mac-address* **vlan** *vlan-id*

- *mac-address* - MAC address.
- *interface*
 - **ethernet** *unit/port*
 - *unit* - This is device 1.
 - *port* - Port number.
 - **port-channel** *channel-id* (Range: 1-4)
- *vlan-id* - VLAN ID (Range: 1-4094)

- *action* -
 - **delete-on-reset** - Assignment lasts until the switch is reset.
 - **permanent** - Assignment is permanent.

Default Setting

No static addresses are defined. The default mode is **permanent**.

Command Mode

Global Configuration

Command Usage

The static address for a host device can be assigned to a specific port within a specific VLAN. Use this command to add static addresses to the MAC Address Table. Static addresses have the following characteristics:

- Static addresses will not be removed from the address table when a given interface link is down.
- Static addresses are bound to the assigned interface and will not be moved. When a static address is seen on another interface, the address will be ignored and will not be written to the address table.
- A static address cannot be learned on another port until the address is removed with the **no** form of this command.

Example

```
Console(config)#mac-address-table static 00-e0-29-94-34-de interface  
ethernet 1/1 vlan 1 delete-on-reset  
Console(config)#
```

clear mac-address-table dynamic

Use this command to remove any learned entries from the forwarding database and to clear the transmit and receive counts for any static or system configured entries.

Default Setting

None

Command Mode

Privileged Exec

Example

```
Console#clear mac-address-table dynamic
Console#
```

show mac-address-table

Use this command to view classes of entries in the bridge-forwarding database.

Syntax

show mac-address-table [**address** *mac-address* [*mask*]] [**interface** *interface*] [**vlan** *vlan-id*] [**sort** {**address** | **vlan** | **interface**}]

- *mac-address* - MAC address.
- *mask* - Bits to match in the address.
- *interface*
 - **ethernet** *unit/port*
 - *unit* - This is device 1.
 - *port* - Port number.
 - **port-channel** *channel-id* (Range: 1-4)
- *vlan-id* - VLAN ID (Range: 1-4094)
- **sort** - Sort by address, vlan or interface.

Default Setting

None

Command Mode

Privileged Exec

Command Usage

- The MAC Address Table contains the MAC addresses associated with each interface. Note that the Type field may include the following types:
 - Learned - Dynamic address entries
 - Permanent - Static entry
 - Delete-on-reset - Static entry to be deleted when system is reset
- The mask should be hexadecimal numbers (representing an equivalent bit mask) in the form xx-xx-xx-xx-xx-xx that is applied to the specified MAC address. Enter hexadecimal numbers, where an equivalent binary bit “0” means to match a bit and “1” means to ignore a bit. For example, a mask of 00-00-00-00-00-00 means an exact match, and a mask of FF-FF-FF-FF-FF-FF means “any.”
- The maximum number of address entries is 8191.

Example

```
Console#show mac-address-table
  Interface Mac Address          Vlan Type
  -----
  Eth 1/ 1  00-e0-29-94-34-de    1 Delete-on-reset
Console#
```

mac-address-table aging-time

Use this command to set the aging time for entries in the address table.
Use the **no** form to restore the default aging time.

Syntax

mac-address-table aging-time *seconds*
no mac-address-table aging-time
seconds - Time in number of seconds (10-1000000).

Default Setting

300 seconds

Command Mode

Global Configuration

Command Usage

The aging time is used to age out dynamically learned forwarding information.

Example

```
Console(config)#mac-address-table aging-time 100
Console(config)#
```

show mac-address-table aging-time

Use this command to show the aging time for entries in the address table.

Default Setting

None

Command Mode

Privileged Exec

Example

```
Console#show mac-address-table aging-time
Aging time: 300 sec.
Console#
```

Spanning Tree Commands

This section includes commands that configure the Spanning Tree Algorithm (STA) globally for the switch, and commands that configure STA for the selected interface.

Command	Function	Mode	Page
spanning-tree	Enables the spanning tree protocol	GC	4-147
spanning-tree mode	Configures STP or RSTP mode	GC	4-148
spanning-tree forward-time	Configures the spanning tree bridge forward time	GC	4-149
spanning-tree hello-time	Configures the spanning tree bridge hello time	GC	4-150
spanning-tree max-age	Configures the spanning tree bridge maximum age	GC	4-150
spanning-tree priority	Configures the spanning tree bridge priority	GC	4-151
spanning-tree path-cost method	Configures the path cost method for RSTP	GC	4-152
spanning-tree transmission-limit	Configures the transmission limit for RSTP	GC	4-153
spanning-tree cost	Configures the spanning tree path cost of an interface	IC	4-154
spanning-tree port-priority	Configures the spanning tree priority of an interface	IC	4-155
spanning-tree edge-port	Enables fast forwarding for edge ports	IC	4-156
spanning-tree portfast	Sets an interface to fast forwarding	IC	4-157
spanning-tree link-type	Configures the link type for RSTP	IC	4-158
spanning-tree protocol-migration	Re-checks the appropriate BPDU format	PE	4-159
show spanning-tree	Shows spanning tree configuration for the overall bridge or a selected interface	PE	4-160

spanning-tree

Use this command to enable the Spanning Tree Algorithm globally for the switch. Use the **no** form to disable it.

Syntax

spanning-tree
no spanning-tree

Default Setting

Spanning tree is enabled.

Command Mode

Global Configuration

Command Usage

The Spanning Tree Algorithm (STA) can be used to detect and disable network loops, and to provide backup links between switches, bridges or routers. This allows the switch to interact with other bridging devices (that is, an STA-compliant switch, bridge or router) in your network to ensure that only one route exists between any two stations on the network, and provide backup links which automatically take over when a primary link goes down.

Example

This example shows how to enable the Spanning Tree Algorithm for the switch:

```
Console(config)#spanning-tree
Console(config)#
```

spanning-tree mode

Use this command to select the spanning tree mode for this switch. Use the **no** form to restore the default.

Syntax

spanning-tree mode {stp | rstp}

no spanning-tree mode

- **stp** - Spanning Tree Protocol (IEEE 802.1D)
- **rstp** - Rapid Spanning Tree Protocol (IEEE 802.1w)

Default Setting

rstp

Command Mode

Global Configuration

Command Usage

- Spanning Tree Protocol
Uses RSTP for the internal state machine, but sends only 802.1D BPDUs.
- Rapid Spanning Tree Protocol
RSTP supports connections to either STP or RSTP nodes by monitoring the incoming protocol messages and dynamically adjusting the type of protocol messages the RSTP node transmits, as described below:
 - STP Mode – If the switch receives an 802.1D BPDU after a port's migration delay timer expires, the switch assumes it is connected to an 802.1D bridge and starts using only 802.1D BPDUs.
 - RSTP Mode – If RSTP is using 802.1D BPDUs on a port and receives an RSTP BPDU after the migration delay expires, RSTP restarts the migration delay timer and begins using RSTP BPDUs on that port.

Example

The following example configures the switch to use Rapid Spanning Tree:

```
Console(config)#spanning-tree mode rstp
Console(config)#
```

spanning-tree forward-time

Use this command to configure the spanning tree bridge forward time globally for this switch. Use the **no** form to restore the default.

Syntax

spanning-tree forward-time *seconds*

no spanning-tree forward-time

seconds - Time in seconds. (Range: 4 - 30 seconds)

The minimum value is the higher of 4 or $[(\text{max-age} / 2) + 1]$.

Default Setting

15 seconds

Command Mode

Global Configuration

Command Usage

This command sets the maximum time (in seconds) the root device will wait before changing states (i.e., discarding to learning to forwarding). This delay is required because every device must receive information about topology changes before it starts to forward frames. In addition, each port needs time to listen for conflicting information that would make it return to the discarding state; otherwise, temporary data loops might result.

Example

```
Console(config)#spanning-tree forward-time 20
Console(config)#
```

spanning-tree hello-time

Use this command to configure the spanning tree bridge hello time globally for this switch. Use the **no** form to restore the default.

Syntax

spanning-tree hello-time *time*

no spanning-tree hello-time

time - Time in seconds. (Range: 1-10 seconds).

The maximum value is the lower of 10 or $[(\text{max-age} / 2) - 1]$.

Default Setting

2 seconds

Command Mode

Global Configuration

Command Usage

This command sets the time interval (in seconds) at which the root device transmits a configuration message.

Example

```
Console(config)#spanning-tree hello-time 5
Console(config)#
```

spanning-tree max-age

Use this command to configure the spanning tree bridge maximum age globally for this switch. Use the **no** form to restore the default.

Syntax

spanning-tree max-age *seconds*

no spanning-tree max-age

seconds - Time in seconds. (Range: 6-40 seconds)

The minimum value is the higher of 6 or $[2 \times (\text{hello-time} + 1)]$.

The maximum value is the lower of 40 or $[2 \times (\text{forward-time} - 1)]$.

Default Setting

20 seconds

Command Mode

Global Configuration

Command Usage

This command sets the maximum time (in seconds) a device can wait without receiving a configuration message before attempting to reconfigure. All device ports (except for designated ports) should receive configuration messages at regular intervals. Any port that ages out STA information (provided in the last configuration message) becomes the designated port for the attached LAN. If it is a root port, a new root port is selected from among the device ports attached to the network.

Example

```
Console(config)#spanning-tree max-age 40
Console(config)#
```

spanning-tree priority

Use this command to configure the spanning tree priority globally for this switch. Use the **no** form to restore the default.

Syntax**spanning-tree priority** *priority***no spanning-tree priority***priority* - Priority of the bridge. (Range: 0 - 65535)

(Range – 0-61440, in steps of 4096; Options: 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, 61440)

Default Setting

32768

Command Mode

Global Configuration

Command Usage

Bridge priority is used in selecting the root device, root port, and designated port. The device with the highest priority becomes the STA root device. However, if all devices have the same priority, the device with the lowest MAC address will then become the root device.

Example

```
Console(config)#spanning-tree priority 40000
Console(config)#
```

spanning-tree pathcost method

Use this command to configure the path cost method used for Rapid Spanning Tree. Use the **no** form to restore the default.

Syntax

spanning-tree pathcost method {long | short}

no spanning-tree pathcost method

- **long** - Specifies 32-bit based values that range from 1-200,000,000.
- **short** - Specifies 16-bit based values that range from 1-65535.

Default Setting

Long method

Command Mode

Global Configuration

Command Usage

The path cost method is used to determine the best path between devices. Therefore, lower values should be assigned to ports attached to faster media, and higher values assigned to ports with slower media. Note that path cost (page 4-154) takes precedence over port priority (page 4-155).

Example

```
Console(config)#spanning-tree pathcost method long
Console(config)#
```

spanning-tree transmission-limit

Use this command to configure the minimum interval between the transmission of consecutive RSTP BPDUs. Use the **no** form to restore the default.

Syntax

spanning-tree transmission-limit *count*

no spanning-tree transmission-limit

count - The transmission limit in seconds. (Range: 1-10)

Default Setting

3

Command Mode

Global Configuration

Command Usage

This command limits the maximum transmission rate for BPDUs.

Example

```
Console(config)#spanning-tree transmission-limit 4
Console(config)#
```

spanning-tree cost

Use this command to configure the spanning tree path cost for the specified interface. Use the **no** form to restore the default.

Syntax

spanning-tree cost *cost*

no spanning-tree cost

cost - The path cost for the port. (Range: 1-200,000,000)

The recommended range is:

- Ethernet: 200,000-20,000,000
- Fast Ethernet: 20,000-2,000,000
- Gigabit Ethernet: 2,000-200,000

Default Setting

- Ethernet – half duplex: 2,000,000; full duplex: 1,000,000; trunk: 500,000
- Fast Ethernet – half duplex: 200,000; full duplex: 100,000; trunk: 50,000
- Gigabit Ethernet – full duplex: 10,000; trunk: 5,000

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- This command is used by the Spanning Tree Algorithm to determine the best path between devices. Therefore, lower values should be assigned to ports attached to faster media, and higher values assigned to ports with slower media.
- Path cost takes precedence over port priority.
- When the spanning-tree pathcost method (page 4-152) is set to short, the maximum value for path cost is 65,535.

Example

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree cost 50
Console(config-if)#
```


spanning-tree port-priority

Use this command to configure the priority for the specified interface. Use the **no** form to restore the default.

Syntax

spanning-tree port-priority *priority*

no spanning-tree port-priority

priority - The priority for a port. (Range: 0-240, in steps of 16)

Default Setting

128

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- This command defines the priority for the use of a port in the Spanning Tree Algorithm. If the path cost for all ports on a switch are the same, the port with the highest priority (that is, lowest value) will be configured as an active link in the spanning tree.
- Where more than one port is assigned the highest priority, the port with lowest numeric identifier will be enabled.

Example

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree port-priority 0
Console(config-if)#
```

Related Commands

spanning-tree cost (4-154)

spanning-tree edge-port

Use this command to specify an interface as an edge port. Use the **no** form to restore the default.

Syntax

spanning-tree edge-port
no spanning-tree edge-port

Default Setting

Disabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- You can enable this option if an interface is attached to a LAN segment that is at the end of a bridged LAN or to an end node. Since end nodes cannot cause forwarding loops, they can pass directly through to the spanning tree forwarding state. Specifying Edge Ports provides quicker convergence for devices such as workstations or servers, retains the current forwarding database to reduce the amount of frame flooding required to rebuild address tables during reconfiguration events, does not cause the spanning tree to initiate reconfiguration when the interface changes state, and also overcomes other STA-related timeout problems. However, remember that Edge Port should only be enabled for ports connected to an end-node device.
- This command has the same effect as the **spanning-tree portfast**.

Example

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree edge-port
Console(config-if)#
```

Related Commands

spanning-tree portfast (4-157)

spanning-tree portfast

Use this command to set an interface to fast forwarding. Use the **no** form to disable fast forwarding.

Syntax

spanning-tree portfast
no spanning-tree portfast

Default Setting

Disabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- This command is used to enable/disable the fast spanning-tree mode for the selected port. In this mode, ports skip the Discarding and Learning states, and proceed straight to Forwarding.
- Since end-nodes cannot cause forwarding loops, they can be passed through the spanning tree state changes more quickly than allowed by standard convergence time. Fast forwarding can achieve quicker convergence for end-node workstations and servers, and also overcome other STA related timeout problems. (Remember that fast forwarding should only be enabled for ports connected to a LAN segment that is at the end of a bridged LAN or for an end-node device.)
- This command is the same as **spanning-tree edge-port**, and is only included for backward compatibility with earlier products. Note that this command may be removed for future software versions.

Example

```
Console(config)#interface ethernet 1/5
Console(config-if)#bridge-group 1 portfast
Console(config-if)#
```

Related Commands

spanning-tree edge-port (4-156)

spanning-tree link-type

Use this command to configure the link type for Rapid Spanning Tree. Use the **no** form to restore the default.

Syntax

spanning-tree link-type {auto | point-to-point | shared}
no spanning-tree link-type

- **auto** - Automatically derived from the duplex mode setting.
- **point-to-point** - Point-to-point link.
- **shared** - Shared medium.

Default Setting

auto

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- Specify a point-to-point link if the interface can only be connected to exactly one other bridge, or a shared link if it can be connected to two or more bridges.
- When automatic detection is selected, the switch derives the link type from the duplex mode. A full-duplex interface is considered a point-to-point link, while a half-duplex interface is assumed to be on a shared link.
- RSTP only works on point-to-point links between two bridges. If you designate a port as a shared link, RSTP is forbidden.

Example

```
Console(config)#interface ethernet SNP5
Console(config-if)#spanning-tree link-type point-to-point
Console(config-if)#
```

spanning-tree protocol-migration

Use this command to re-check the appropriate BPDU format to send on the selected interface.

Syntax

spanning-tree protocol-migration *interface*

interface

- **ethernet** *unit/port*
 - *unit* - This is device 1.
 - *port* - Port number.
- **port-channel** *channel-id* (Range: 1-6)

Command Mode

Privileged Exec

Command Usage

If at any time the switch detects STP BPDUs, including Configuration or Topology Change Notification BPDUs, it will automatically set the selected interface to forced STP-compatible mode. However, you can also use the **spanning-tree protocol-migration** command at any time to manually re-check the appropriate BPDU format to send on the selected interfaces (i.e., RSTP or STP-compatible).

Example

```
Console(config)#interface ethernet SNP5
Console(config-if)#spanning-tree protocol-migration
Console(config-if)#
```

show spanning-tree

Use this command to show the spanning tree configuration.

Syntax

show spanning-tree [*interface*]

interface

- **ethernet** *unit/port*
 - *unit* - This is device 1.
 - *port* - Port number.
- **port-channel** *channel-id* (Range: 1-4)

Default Setting

None

Command Mode

Privileged Exec

Command Usage

- Use the **show spanning-tree** command with no parameters to display the spanning tree configuration for the switch and for every interface in the tree.
- Use the **show spanning-tree** *interface* command to display the spanning tree configuration for an interface.
- For a description of the items displayed under “Spanning-tree information,” see “Configuring Global Settings” on page -92. For a description of the items displayed for specific interfaces, see “Displaying Interface Settings” on page -95.

Example

```

Console#show spanning-tree
Spanning-tree information
-----
Spanning tree mode           :RSTP
Spanning tree enable/disable :enable
Priority                     :32768
Bridge Hello Time (sec.)    :2
Bridge Max Age (sec.)       :20
Bridge Forward Delay (sec.) :15
Root Hello Time (sec.)      :2
Root Max Age (sec.)         :20
Root Forward Delay (sec.)   :15
Designated Root             :32768.0000ABCD0000
Current root port           :0
Current root cost            :0
Number of topology changes  :2
Last topology changes time (sec.):1718
Transmission limit          :3
Path Cost Method             :long
-----
Eth 1/ 1 information
-----
Admin status      : enable
Role              : disable
State             : discarding
Path cost         : 100000
Priority          : 128
Designated cost   : 0
Designated port   : 128.1
Designated root   : 32768.0000ABCD0000
Designated bridge : 32768.0000ABCD0000
Forward transitions : 0
Fast forwarding   : disable
Admin edge port   : disable
Oper edge port    : disable
Admin Link type   : auto
Oper Link type    : point-to-point
.
.
.
Console#

```

VLAN Commands

A VLAN is a group of ports that can be located anywhere in the network, but communicate as though they belong to the same physical segment. This section describes commands used to create VLAN groups, add port members, specify how VLAN tagging is used, and enable automatic VLAN registration for the selected interface.

Command Groups	Function	Page
Editing VLAN Groups	Sets up VLAN groups, including name, VID and state	4-162
Configuring VLAN Interfaces	Configures VLAN interface parameters, including ingress and egress tagging mode, ingress filtering, PVID, and GVRP	4-164
Displaying VLAN Information	Displays VLAN groups, status, port members, and MAC addresses	4-172
Configuring Private VLANs	Configures private VLANs, including uplink and downlink ports	4-173

Editing VLAN Groups

Command	Function	Mode	Page
vlan database	Enters VLAN database mode to add, change, and delete VLANs	GC	4-162
vlan	Configures a VLAN, including VID, name and state	VC	4-163

vlan database

Use this command to enter VLAN database mode. All commands in this mode will take effect immediately.

Default Setting

None

Command Mode

Global Configuration

Command Usage

- Use the VLAN database command mode to add, change, and delete VLANs. After finishing configuration changes, you can display the VLAN settings by entering the **show vlan** command.
- Use the **interface vlan** command mode to define the port membership mode and add or remove ports from a VLAN. The results of these commands are written to the running-configuration file, and you can display this file by entering the **show running-config** command.

Example

```
Console(config)#vlan database
Console(config-vlan)#
```

Related Commands

show vlan (4-172)

vlan

Use this command to configure a VLAN. Use the **no** form to restore the default settings or delete a VLAN.

Syntax

vlan *vlan-id* [**name** *vlan-name*] **media ethernet** [**state** {**active** | **suspend**}]

no vlan *vlan-id* [**name** | **state**]

- *vlan-id* - ID of configured VLAN. (Range: 1-4094, no leading zeroes)
- **name** - Keyword to be followed by the VLAN name.
 - *vlan-name* - ASCII string from 1 to 32 characters.
- **media ethernet** - Ethernet media type.
- **state** - Keyword to be followed by the VLAN state.
 - **active** - VLAN is operational.
 - **suspend** - VLAN is suspended. Suspended VLANs do not pass packets.

Default Setting

By default only VLAN 1 exists and is active.

Command Mode

VLAN Database Configuration

Command Usage

- **no vlan *vlan-id*** deletes the VLAN.
- **no vlan *vlan-id* name** removes the VLAN name.
- **no vlan *vlan-id* state** returns the VLAN to the default state (i.e., active).
- You can configure up to 255 VLANs on the switch.

Example

The following example adds a VLAN, using VLAN ID 105 and name RD5. The VLAN is activated by default.

```
Console(config)#vlan database
Console(config-vlan)#vlan 105 name RD5 media ethernet
Console(config-vlan)#
```

Related Commands

show vlan (4-172)

Configuring VLAN Interfaces

Command	Function	Mode	Page
interface vlan	Enters interface configuration mode for a specified VLAN	IC	4-165
switchport mode	Configures VLAN membership mode for an interface	IC	4-166
switchport acceptable-frame-types	Configures frame types to be accepted by an interface	IC	4-167
switchport ingress-filtering	Enables ingress filtering on an interface	IC	4-168
switchport native vlan	Configures the PVID (native VLAN) of an interface	IC	4-169

Command	Function	Mode	Page
switchport allowed vlan	Configures the VLANs associated with an interface	IC	4-170
switchport gvrp	Enables GVRP for an interface	IC	4-177
switchport forbidden vlan	Configures forbidden VLANs for an interface	IC	4-171

interface vlan

Use this command to enter interface configuration mode for VLANs, and configure a physical interface.

Syntax

interface vlan *vlan-id*

vlan-id - ID of the configured VLAN.

(Range: 1-4094, no leading zeroes)

Default Setting

None

Command Mode

Global Configuration

Example

The following example shows how to set the interface configuration mode to VLAN 1, and then assign an IP address to the VLAN:

```
Console(config)#interface vlan 1
Console(config-if)#ip address 192.168.1.254 255.255.255.0
Console(config-if)#
```

Related Commands

shutdown (4-125)

switchport mode

Use this command to configure the VLAN membership mode for a port. Use the **no** form to restore the default.

Syntax

switchport mode {trunk | hybrid}
no switchport mode

- **trunk** - Specifies a port as an end-point for a VLAN trunk. A trunk is a direct link between two switches, so the port transmits tagged frames that identify the source VLAN. However, note that frames belonging to the port's default VLAN (i.e., associated with the PVID) are sent untagged.
- **hybrid** - Specifies a hybrid VLAN interface. The port may transmit tagged or untagged frames.

Default Setting

All ports are in hybrid mode with the PVID set to VLAN 1.

Command Mode

Interface Configuration (Ethernet, Port Channel)

Example

The following shows how to set the configuration mode to port 1, and then set the switchport mode to hybrid:

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport mode hybrid
Console(config-if)#
```

Related Commands

switchport acceptable-frame-types (4-167)

switchport acceptable-frame-types

Use this command to configure the acceptable frame types for a port. Use the **no** form to restore the default.

Syntax

switchport acceptable-frame-types {all | tagged}

no switchport acceptable-frame-types

- **all** - The port accepts all frames, tagged or untagged.
- **tagged** - The port only receives tagged frames.

Default Setting

All frame types

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

When set to receive all frame types, any received frames that are untagged are assigned to the default VLAN.

Example

The following example shows how to restrict the traffic received on port 1 to tagged frames:

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport acceptable-frame-types tagged
Console(config-if)#
```

Related Commands

switchport mode (4-166)

switchport ingress-filtering

Use this command to enable ingress filtering for an interface. Use the **no** form to restore the default.

Syntax

switchport ingress-filtering
no switchport ingress-filtering

Default Setting

Disabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- Ingress filtering only affects tagged frames.
- If ingress filtering is disabled and a port receives frames tagged for VLANs for which it is not a member, these frames will be flooded to all other ports (except for those VLANs explicitly forbidden on this port).
- If ingress filtering is enabled and a port receives frames tagged for VLANs for which it is not a member, these frames will be discarded.
- Ingress filtering does not affect VLAN independent BPDU frames, such as GVRP or STA. However, they do affect VLAN dependent BPDU frames, such as GMRP.

Example

The following example shows how to set the interface to port 1 and then enable ingress filtering:

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport ingress-filtering
Console(config-if)#
```

switchport native vlan

Use this command to configure the PVID (i.e., default VLAN ID) for a port. Use the **no** form to restore the default.

Syntax

switchport native vlan *vlan-id*

no switchport native vlan

vlan-id - Default VLAN ID for a port. (Range: 1-4094, no leading zeroes)

Default Setting

VLAN 1

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- If an interface is not a member of VLAN 1 and you assign its PVID to this VLAN, the interface will automatically be added to VLAN 1 as an untagged member. For all other VLANs, an interface must first be configured as an untagged member before you can assign its PVID to that group.
- If acceptable frame types is set to **all** or switchport mode is set to **hybrid**, the PVID will be inserted into all untagged frames entering the ingress port.

Example

The following example shows how to set the PVID for port 1 to VLAN 3:

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport native vlan 3
Console(config-if)#
```

switchport allowed vlan

Use this command to configure VLAN groups on the selected interface.
Use the **no** form to restore the default.

Syntax

switchport allowed vlan {**add** *vlan-list* [**tagged** | **untagged**] |
remove *vlan-list*}

no switchport allowed vlan

- **add** *vlan-list* - List of VLAN identifiers to add.
- **remove** *vlan-list* - List of VLAN identifiers to remove.
- *vlan-list* - Separate nonconsecutive VLAN identifiers with a comma and no spaces; use a hyphen to designate a range of IDs. Do not enter leading zeros. (Range: 1-4094).

Default Setting

All ports are assigned to VLAN 1 by default.
The default frame type is untagged.

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- A port, or a trunk with switchport mode set to **hybrid**, must be assigned to at least one VLAN as untagged.
- If a trunk has switchport mode set to **trunk** (i.e., 1Q Trunk), then you can only assign an interface to VLAN groups as a tagged member.
- Frames are always tagged within the switch. The tagged/untagged parameter used when adding a VLAN to an interface tells the switch whether to keep or remove the tag from a frame on egress.
- If none of the intermediate network devices nor the host at the other end of the connection supports VLANs, the interface should be added to these VLANs as an untagged member. Otherwise, it is only necessary to add at most one VLAN as untagged, and this should correspond to the native VLAN for the interface.

- If a VLAN on the forbidden list for an interface is manually added to that interface, the VLAN is automatically removed from the forbidden list for that interface.

Example

The following example shows how to add VLANs 1, 2, 5 and 6 to the allowed list as tagged VLANs for port 1:

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport allowed vlan add 1,2,5,6 tagged
Console(config-if)#
```

switchport forbidden vlan

Use this command to configure forbidden VLANs. Use the **no** form to remove the list of forbidden VLANs.

Syntax

switchport forbidden vlan {add *vlan-list* | remove *vlan-list*}
no switchport forbidden vlan

- **add *vlan-list*** - List of VLAN identifiers to add.
- **remove *vlan-list*** - List of VLAN identifiers to remove.
- *vlan-list* - Separate nonconsecutive VLAN identifiers with a comma and no spaces; use a hyphen to designate a range of IDs. Do not enter leading zeros. (Range: 1-4094).

Default Setting

No VLANs are included in the forbidden list.

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- This command prevents a VLAN from being automatically added to the specified interface via GVRP.
- If a VLAN has been added to the set of allowed VLANs for an interface, then you cannot add it to the set of forbidden VLANs for that same interface.

Example

The following example shows how to prevent port 1 from being added to VLAN 3:

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport forbidden vlan add 3
Console(config-if)#
```

Displaying VLAN Information

Command	Function	Mode	Page
show vlan	Shows VLAN information	NE, PE	4-172
show interfaces status vlan	Displays status for the specified VLAN interface	NE, PE	4-128
show interfaces switchport	Displays the administrative and operational status of an interface	NE, PE	4-131

show vlan

Use this command to show VLAN information.

Syntax

show vlan [**id** *vlan-id* | **name** *vlan-name*]

- **id** - Keyword to be followed by the VLAN ID.
 - *vlan-id* - ID of the configured VLAN. (Range: 1-4094, no leading zeroes)
- **name** - Keyword to be followed by the VLAN name.
 - *vlan-name* - ASCII string from 1 to 32 characters.

Default Setting

Shows all VLANs.

Command Mode

Normal Exec, Privileged Exec

Example

The following example shows how to display information for VLAN 1:

```

Console#show vlan id 1
VLAN Type      Name        Status        Ports/Channel groups
-----
 1  Static      DefaultVlan  Active        Eth1/ 1 Eth1/ 2 Eth1/ 3 Eth1/ 4 Eth1/ 5
                        Eth1/ 6 Eth1/ 7 Eth1/ 8 Eth1/ 9 Eth1/10
                        Eth1/11 Eth1/12 Eth1/13 Eth1/14 Eth1/15
                        Eth1/16 Eth1/17 Eth1/18 Eth1/19 Eth1/20
                        Eth1/21 Eth1/22 Eth1/23 Eth1/24 Eth1/25
                        Eth1/26
Console#

```

Configuring Private VLANs

Private VLANs provide port-based security and isolation between ports within the assigned VLAN. This section describes commands used to configure private VLANs.

Command	Function	Mode	Page
pvlan	Enables and configured private VLANS	GC	4-173
show pvlan	Displays the configured private VLANS	PE	4-174

pvlan

Use this command to enable or configure a private VLAN. Use the **no** form to disable the private VLAN.

Syntax

```

pvlan [up-link interface-list down-link interface-list]
no pvlan

```

- **up-link** – Specifies an uplink interface.
- **down-link** – Specifies a downlink interface.

Default Setting

No private VLANs are defined.

Command Mode

Global Configuration

Command Usage

- A private VLAN provides port-based security and isolation between ports within the VLAN. Data traffic on the downlink ports can only be forwarded to, and from, the uplink port.
- Private VLANs and normal VLANs can exist simultaneously within the same switch.
- Entering the **pvlan** command without any parameters enables the private VLAN. Entering **no pvlan** disables the private VLAN.

Example

This example enables the private VLAN, and then sets port 25 as the uplink and ports 1-8 as the downlinks.

```
Console(config)#pvlan
Console(config)#pvlan up-link ethernet 1/25 down-link ethernet 1/1-8
Console(config)#
```

show pvlan

Use this command to display the configured private VLAN.

Command Mode

Privileged Exec

Example

```
Console#show pvlan
Private VLAN status: Enabled
Up-link port:
  Ethernet 1/25
Down-link port:
  Ethernet 1/1-8
Console#
```

GVRP and Bridge Extension Commands

GARP VLAN Registration Protocol defines a way for switches to exchange VLAN information in order to automatically register VLAN members on interfaces across the network. This section describes how to enable GVRP for individual interfaces and globally for the switch, as well as how to display default configuration settings for the Bridge Extension MIB.

Command	Function	Mode	Page
bridge-ext gvrp	Enables GVRP globally for the switch	GC	4-175
show bridge-ext	Shows the global bridge extension configuration	PE	4-176
switchport gvrp	Enables GVRP for an interface	IC	4-177
switchport forbidden vlan	Configures forbidden VLANs for an interface	IC	4-171
show gvrp configuration	Displays GVRP configuration for the selected interface	NE, PE	4-178
garp timer	Sets the GARP timer for the selected function	IC	4-178
show garp timer	Shows the GARP timer for the selected function	NE, PE	4-180

bridge-ext gvrp

Use this command to enable GVRP globally for the switch. Use the **no** form to disable it.

Syntax

```
bridge-ext gvrp
no bridge-ext gvrp
```

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

GVRP defines a way for switches to exchange VLAN information in order to register VLAN members on ports across the network. This function should be enabled to permit automatic VLAN registration, and to support VLANs which extend beyond the local switch.

Example

```
Console(config)#bridge-ext gvrp
Console(config)#
```

show bridge-ext

Use this command to show the configuration for bridge extension commands.

Default Setting

None

Command Mode

Privileged Exec

Command Usage

See “Displaying Basic VLAN Information” on page -107 and “Displaying Bridge Extension Capabilities” on page -16 for a description of the displayed items.

Example

```
Console#show bridge-ext
Max support vlan numbers: 255
Max support vlan ID: 4094
Extended multicast filtering services: No
Static entry individual port: Yes
VLAN learning: IVL
Configurable PVID tagging: Yes
Local VLAN capable: No
Traffic classes: Enabled
Global GVRP status: Disabled
GMRP: Disabled
Console#
```

switchport gvrp

Use this command to enable GVRP for a port. Use the **no** form to disable it.

Syntax

```
switchport gvrp
no switchport gvrp
```

Default Setting

Disabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport gvrp
Console(config-if)#
```

show gvrp configuration

Use this command to show if GVRP is enabled.

Syntax

show gvrp configuration [*interface*]

interface

- **ethernet** *unit/port*
 - *unit* - This is device 1.
 - *port* - Port number.
- **port-channel** *channel-id* (Range: 1-6)

Default Setting

Shows both global and interface-specific configuration.

Command Mode

Normal Exec, Privileged Exec

Example

```
Console#show gvrp configuration ethernet 1/7
Eth 1/ 7:
  Gvrp configuration: Disabled
Console#
```

garp timer

Use this command to set the values for the join, leave and leaveall timers.

Use the **no** form to restore the timers' default values.

Syntax

garp timer {**join** | **leave** | **leaveall**} *timer_value*

no garp timer {**join** | **leave** | **leaveall**}

- {**join** | **leave** | **leaveall**} - Which timer to set.
- *timer_value* - Value of timer.

Ranges:

join: 20-1000 centiseconds

leave: 60-3000 centiseconds

leaveall: 500-18000 centiseconds

Default Setting

- join: 20 centiseconds
- leave: 60 centiseconds
- leaveall: 1000 centiseconds

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- Group Address Registration Protocol is used by GVRP and GMRP to register or deregister client attributes for client services within a bridged LAN. The default values for the GARP timers are independent of the media access method or data rate. These values should not be changed unless you are experiencing difficulties with GMRP or GVRP registration/deregistration.
- Timer values are applied to GVRP for all the ports on all VLANs.
- Timer values must meet the following restrictions:
 - leave \geq (2 x join)
 - leaveall > leave

Note: Set GVRP timers on all Layer 2 devices connected in the same network to the same values. Otherwise, GVRP may not operate successfully.

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#garp timer join 100
Console(config-if)#
```

Related Commands

show garp timer (4-180)

show garp timer

Use this command to show the GARP timers for the selected interface.

Syntax

show garp timer [*interface*]

interface

- **ethernet** *unit/port*
 - *unit* - This is device 1.
 - *port* - Port number.
- **port-channel** *channel-id* (Range: 1-6)

Default Setting

Shows all GARP timers.

Command Mode

Normal Exec, Privileged Exec

Example

```
Console#show garp timer ethernet 1/1
Eth 1/ 1 GARP timer status:
Join timer: 20 centiseconds
Leave timer: 60 centiseconds
Leaveall timer: 1000 centiseconds
Console#
```

Related Commands

garp timer (4-178)

Priority Commands

The commands described in this section allow you to specify which data packets have greater precedence when traffic is buffered in the switch due to congestion. This switch supports CoS with four priority queues for each port. Data packets in a port's high-priority queue will be transmitted before those in the lower-priority queues. You can set the default priority for each interface, the relative weight of each queue, and the mapping of frame priority tags to the switch's priority queues.

Command Groups	Function	Page
Priority (Layer 2)	Configures default priority for untagged frames, sets queue weights, and maps class of service tags to hardware queues	4-181
Priority (Layer 3 and 4)	Maps TCP ports, IP precedence tags, or IP DSCP tags to class of service values	4-187

Priority Commands (Layer 2)

Command	Function	Mode	Page
switchport priority default	Sets a port priority for incoming untagged frames	IC	4-182
queue bandwidth	Assigns round-robin weights to the priority queues	GC	4-183
queue cos map	Assigns class-of-service values to the priority queues	IC	4-184
show queue bandwidth	Shows round-robin weights assigned to the priority queues	PE	4-185
show queue cos-map	Shows the class-of-service map	PE	4-186
show interfaces switchport	Displays the administrative and operational status of an interface	PE	4-131

switchport priority default

Use this command to set a priority for incoming untagged frames. Use the **no** form to restore the default value.

Syntax

switchport priority default *default-priority-id*

no switchport priority default

default-priority-id - The priority number for untagged ingress traffic. The priority is a number from 0 to 7. Seven is the highest priority.

Default Setting

The priority is not set, and the default value for untagged frames received on the interface is zero.

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- The precedence for priority mapping is IP Port, IP Precedence or IP DSCP, and default switchport priority.
- The default priority applies for an untagged frame received on a port set to accept all frame types (i.e, receives both untagged and tagged frames). This priority does not apply to IEEE 802.1Q VLAN tagged frames. If the incoming frame is an IEEE 802.1Q VLAN tagged frame, the IEEE 802.1p User Priority bits will be used.
- This switch provides four priority queues for each port. It is configured to use Weighted Round Robin, which can be viewed with the **show queue bandwidth** command. Inbound frames that do not have VLAN tags are tagged with the input port's default ingress user priority, and then placed in the appropriate priority queue at the output port. The default priority for all ingress ports is zero. Therefore, any inbound frames that do not have priority tags will be placed in queue 0 of the output port. (Note that if the output port is an untagged member of the associated VLAN, these frames are stripped of all VLAN tags prior to transmission.)

Example

The following example shows how to set a default priority on port 3 to 5:

```
Console(config)#interface ethernet 1/3
Console(config-if)#switchport priority default 5
```

queue bandwidth

Use this command to assign weighted round-robin (WRR) weights to the four class of service (CoS) priority queues. Use the **no** form to restore the default weights.

Syntax

queue bandwidth *weight1...weight4*

no queue bandwidth

weight1...weight4 - The ratio of weights for queues 0 - 3 determines the weights used by the WRR scheduler. (Range: 1 - 255)

Default Setting

Weights 1, 4, 16 and 64 are assigned to queue 0, 1, 2 and 3 respectively.

Command Mode

Global Configuration

Command Usage

WRR controls bandwidth sharing at the egress port by defining scheduling weights.

Example

The following example shows how to assign WRR weights of 1, 3, 5 and 7 to the CoS priority queues 0, 1, 2 and 3:

```
Console(config)#queue bandwidth 1 3 5 7
Console(config)#
```

Related Commands

show queue bandwidth (4-185)

queue cos-map

Use this command to assign class of service (CoS) values to the priority queues (i.e., hardware output queues 0 - 3). Use the **no** form set the CoS map to the default values.

Syntax

queue cos-map *queue_id* [*cos1* ... *cosn*]

no queue cos-map

- *queue_id* - The ID of the priority queue.
Ranges are 0 to 3, where 3 is the highest priority queue.
- *cos1* .. *cosn* - The CoS values that are mapped to the queue ID. It is a space-separated list of numbers. The CoS value is a number from 0 to 7, where 7 is the highest priority.

Default Setting

This switch supports Class of Service by using four priority queues, with Weighted Round Robin queuing for each port. Eight separate traffic classes are defined in IEEE 802.1p. The default priority levels are assigned according to recommendations in the IEEE 802.1p standard as shown in the following table.

	Queue			
	0	1	2	3
Priority		0		
	1			
	2			
		3		
			4	
			5	
				6
				7

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

CoS assigned at the ingress port is used to select a CoS priority at the egress port.

Example

The following example shows how to map CoS values 0, 1 and 2 to priority queue 0, value 3 to queue 1, values 4 and 5 to queue 2, and values 6 and 7 to queue 3:

```
Console(config)#interface ethernet 1/1
Console(config-if)#queue cos-map 0 0 1 2
Console(config-if)#queue cos-map 1 3
Console(config-if)#queue cos-map 2 4 5
Console(config-if)#queue cos-map 3 6 7
Console(config-if)#
```

Related Commands

show queue cos-map (4-186)

show queue bandwidth

Use this command to display the weighted round-robin (WRR) bandwidth allocation for the four priority queues.

Default Setting

None

Command Mode

Privileged Exec

Example

```
Console#show queue bandwidth
Queue ID Weight
-----
0          1
1          4
2         16
3         64
Console#
```

show queue cos-map

Use this command to show the class of service priority map.

Syntax

show queue cos-map [*interface*]

interface

- **ethernet** *unit/port*
 - *unit* - This is device 1.
 - *port* - Port number.
- **port-channel** *channel-id* (Range: 1-6)

Default Setting

None

Command Mode

Privileged Exec

Example

```
Console#show queue cos-map ethernet 1/11
Information of Eth 1/11
Queue ID Traffic class
-----
0         1 2
1         0 3
2         4 5
3         6 7
Console#
```


Priority Commands (Layer 3 and 4)

Command	Function	Mode	Page
map ip port	Enables TCP/UDP class of service mapping	GC	4-187
map ip port	Maps TCP/UDP socket to a class of service	IC	4-188
map ip precedence	Enables IP precedence class of service mapping	GC	4-189
map ip precedence	Maps IP precedence value to a class of service	IC	4-189
map ip dscp	Enables IP DSCP class of service mapping	GC	4-191
map ip dscp	Maps IP DSCP value to a class of service	IC	4-191
show map ip port	Shows the IP port map	PE	4-193
show map ip precedence	Shows the IP precedence map	PE	4-194
show map ip dscp	Shows the IP DSCP map	PE	4-195

map ip port (Global Configuration)

Use this command to enable IP port mapping (i.e., class of service mapping for TCP/UDP sockets). Use the **no** form to disable IP port mapping.

Syntax

map ip port

no map ip port

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

The precedence for priority mapping is IP Port, IP Precedence or IP DSCP, and default switchport priority.

Example

The following example shows how to enable TCP/UDP port mapping globally:

```
Console(config)#map ip port
Console(config)#
```

map ip port (Interface Configuration)

Use this command to set IP port priority (i.e., TCP/UDP port priority). Use the **no** form to remove a specific setting.

Syntax

map ip port *port-number* **cos** *cos-value*

no map ip port *port-number*

- *port-number* - 16-bit TCP/UDP port number. (Range: 0-65535)
- *cos-value* - Class-of-Service value (Range: 0-7)

Default Setting

None

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- The precedence for priority mapping is IP Port, IP Precedence or IP DSCP, and default switchport priority.
- This command sets the IP port priority for all interfaces.

Example

The following example shows how to map HTTP traffic to CoS value 0:

```
Console(config)#interface ethernet 1/5
Console(config-if)#map ip port 80 cos 0
Console(config-if)#
```

map ip precedence (Global Configuration)

Use this command to enable IP precedence mapping (i.e., IP Type of Service). Use the **no** form to disable IP precedence mapping.

Syntax

```
map ip precedence
no map ip precedence
```

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

- The precedence for priority mapping is IP Port, IP Precedence or IP DSCP, and default switchport priority.
- IP Precedence and IP DSCP cannot both be enabled. Enabling one of these priority types will automatically disable the other type.

Example

The following example shows how to enable IP precedence mapping globally:

```
Console(config)#map ip precedence
Console(config)#
```

map ip precedence (Interface Configuration)

Use this command to set IP precedence priority (i.e., IP Type of Service priority). Use the **no** form to restore the default table.

Syntax

```
map ip precedence ip-precedence-value cos cos-value
no map ip precedence
```

- *precedence-value* - 3-bit precedence value. (Range: 0-7)
- *cos-value* - Class-of-Service value (Range: 0-7)

Default Setting

The list below shows the default priority mapping.

IP Precedence Value	CoS Value
0	0
1	1
2	2
3	3
4	4
5	5
6	6
7	7

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- The precedence for priority mapping is IP Port, IP Precedence or IP DSCP, and default switchport priority.
- IP Precedence values are mapped to default Class of Service values on a one-to-one basis according to recommendations in the IEEE 802.1p standard, and then subsequently mapped to the four hardware priority queues.
- This command sets the IP Precedence for all interfaces.

Example

The following example shows how to map IP precedence value 1 to CoS value 0:

```
Console(config)#interface ethernet 1/5
Console(config-if)#map ip precedence 1 cos 0
Console(config-if)#
```

map ip dscp (Global Configuration)

Use this command to enable IP DSCP mapping (i.e., Differentiated Services Code Point mapping). Use the **no** form to disable IP DSCP mapping.

Syntax

```
map ip dscp
no map ip dscp
```

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

- The precedence for priority mapping is IP Port, IP Precedence or IP DSCP, and default switchport priority.
- IP Precedence and IP DSCP cannot both be enabled. Enabling one of these priority types will automatically disable the other type.

Example

The following example shows how to enable IP DSCP mapping globally:

```
Console(config)#map ip dscp
Console(config)#
```

map ip dscp (Interface Configuration)

Use this command to set IP DSCP priority (i.e., Differentiated Services Code Point priority). Use the **no** form to restore the default table.

Syntax

```
map ip dscp dscp-value cos cos-value
no map ip dscp
```

- *dscp-value* - 8-bit DSCP value. (Range: 0-255)
- *cos-value* - Class-of-Service value (Range: 0-7)

Default Setting

The DSCP default values are defined in the following table. Note that all the DSCP values that are not specified are mapped to CoS value 0.

IP DSCP Value	CoS Value
0	0
8	1
10, 12, 14, 16	2
18, 20, 22, 24	3
26, 28, 30, 32, 34, 36	4
38, 40, 42	5
48	6
46, 56	7

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- The precedence for priority mapping is IP Port, IP Precedence or IP DSCP, and default switchport priority.
- DSCP priority values are mapped to default Class of Service values according to recommendations in the IEEE 802.1p standard, and then subsequently mapped to the four hardware priority queues.
- This command sets the IP DSCP priority for all interfaces.

Example

The following example shows how to map IP DSCP value 1 to CoS value 0:

```
Console(config)#interface ethernet 1/5
Console(config-if)#map ip dscp 1 cos 0
Console(config-if)#
```

show map ip port

Use this command to show the IP port priority map.

Syntax

show map ip port [*interface*]

interface

- **ethernet** *unit/port*
 - *unit* - This is device 1.
 - *port* - Port number.
- **port-channel** *channel-id* (Range: 1-6)

Default Setting

None

Command Mode

Privileged Exec

Example

The following shows that HTTP traffic has been mapped to CoS value 0:

```

Console#show map ip port
TCP port mapping status: disabled

  Port          Port no. COS
  -----
  Eth 1/ 5      80    0
Console#

```

Related Commands

map ip port (Global Configuration) (4-187)

map ip port (Interface Configuration) (4-188)

show map ip precedence

Use this command to show the IP precedence priority map.

Syntax

- show map ip precedence** [*interface*]
- interface*
- **ethernet** *unit/port*
 - *unit* - This is device 1.
 - *port* - Port number.
 - **port-channel** *channel-id* (Range: 1-6)

Default Setting

None

Command Mode

Privileged Exec

Example

```
Console#show map ip precedence ethernet 1/5
Precedence mapping status: disabled

Port          Precedence COS
-----
Eth 1/ 5      0  0
Eth 1/ 5      1  1
Eth 1/ 5      2  2
Eth 1/ 5      3  3
Eth 1/ 5      4  4
Eth 1/ 5      5  5
Eth 1/ 5      6  6
Eth 1/ 5      7  7
Console#
```

Related Commands

- map ip precedence (Global Configuration) (4-189)
- map ip precedence (Interface Configuration) (4-189)

show map ip dscp

Use this command to show the IP DSCP priority map.

Syntax

show map ip dscp [*interface*]

interface

- **ethernet** *unit/port*
 - *unit* - This is device 1.
 - *port* - Port number.
- **port-channel** *channel-id* (Range: 1-6)

Default Setting

None

Command Mode

Privileged Exec

Example

```

Console#show map ip dscp ethernet 1/1
DSCP mapping status: disabled

  Port          DSCP  COS
  -----
  Eth 1/ 1      0      0
  Eth 1/ 1      1      0
  Eth 1/ 1      2      0
  Eth 1/ 1      3      0
.
.
.
  Eth 1/ 1      61     0
  Eth 1/ 1      62     0
  Eth 1/ 1      63     0
Console#

```

Related Commands

map ip dscp (Global Configuration) (4-191)
 map ip dscp (Interface Configuration) (4-191)

Multicast Filtering Commands

This switch uses IGMP (Internet Group Management Protocol) to query for any attached hosts that want to receive a specific multicast service. It identifies the ports containing hosts requesting a service and sends data out to those ports only. It then propagates the service request up to any neighboring multicast switch/router to ensure that it will continue to receive the multicast service.

Note that IGMP query can be enabled globally at Layer 2, or enabled for specific VLAN interfaces at Layer 3. (Layer 2 query is disabled if Layer 3 query is enabled.)

Command Groups	Function	Page
IGMP Snooping	Configures multicast groups via IGMP snooping or static assignment, sets the IGMP version, displays current snooping and query settings, and displays the multicast service and group members	4-196
IGMP Query (Layer 2)	Configures IGMP query parameters for multicast filtering at Layer 2	4-201
IGMP (Layer 3)	Configures the IGMP protocol used with multicast routing	4-205

IGMP Snooping Commands

Command	Function	Mode	Page
ip igmp snooping	Enables IGMP snooping	GC	4-197
ip igmp snooping vlan static	Adds an interface as a member of a multicast group	GC	4-197
ip igmp snooping version	Configures the IGMP version for snooping	GC	4-198
show ip igmp snooping	Shows the IGMP snooping and query configuration	PE	4-199
show mac-address-table multicast	Shows the IGMP snooping MAC multicast list	PE	4-200

ip igmp snooping

Use this command to enable IGMP snooping on this switch. Use the **no** form to disable it.

Syntax

ip igmp snooping
no ip igmp snooping

Default Setting

Enabled

Command Mode

Global Configuration

Example

The following example enables IGMP snooping.

```
Console(config)#ip igmp snooping
Console(config)#
```

ip igmp snooping vlan static

Use this command to add a port to a multicast group. Use the **no** form to remove the port.

Syntax

ip igmp snooping vlan *vlan-id* static *ip-address* *interface*
no ip igmp snooping vlan *vlan-id* static *ip-address* *interface*

- *vlan-id* - VLAN ID (Range: 1-4094)
- *ip-address* - IP address for multicast group
- *interface*
 - **ethernet** *unit/port*
 - *unit* - This is device 1.
 - *port* - Port number.
 - **port-channel** *channel-id* (Range: 1-6)

Default Setting

None

Command Mode

Global Configuration

Example

The following shows how to statically configure a multicast group on a port:

```
Console(config)#ip igmp snooping vlan 1 static 224.0.0.12  
    ethernet 1/5  
Console(config)#
```

ip igmp snooping version

Use this command to configure the IGMP snooping version. Use the **no** form to restore the default.

Syntax

ip igmp snooping version {1 | 2}
no ip igmp snooping version

- **1** - IGMP Version 1
- **2** - IGMP Version 2

Default Setting

IGMP Version 2

Command Mode

Global Configuration

Command Usage

- All systems on the subnet must support the same version. If there are legacy devices in your network that only support Version 1, you will also have to configure this switch to use Version 1.
- Some commands are only enabled for IGMPv2, including **ip igmp query-max-response-time** and **ip igmp query-timeout**.

Example

The following configures the switch to use IGMP Version 1:

```
Console(config)#ip igmp snooping version 1
Console(config)#
```

show ip igmp snooping

Use this command to show the IGMP snooping configuration.

Default Setting

None

Command Mode

Privileged Exec

Command Usage

See “Configuring IGMP Snooping Parameters” on page -137 for a description of the displayed items.

Example

The following shows the current IGMP snooping configuration:

```
Console#show ip igmp snooping
Service status: Enabled
Querier status: Enabled
Query count: 2
Query interval: 125 sec
Query max response time: 10 sec
Query time-out: 300 sec
IGMP snooping version: Version 2
Console#
```

show mac-address-table multicast

Use this command to show known multicast addresses.

Syntax

- show mac-address-table multicast** [**vlan** *vlan-id*]
[**user** | **igmp-snooping**]
- *vlan-id* - VLAN ID (1 to 4094)
 - **user** - Display only the user-configured multicast entries.
 - **igmp-snooping** - Display only entries learned through IGMP snooping.

Default Setting

None

Command Mode

Privileged Exec

Command Usage

Member types displayed include IGMP or USER, depending on selected options.

Example

The following shows the multicast entries learned through IGMP snooping for VLAN 1:

```
Console#show mac-address-table multicast vlan 1 igmp-snooping
VLAN M'cast IP addr. Member ports Type
-----
1      224.1.1.2.3      Eth1/11      IGMP
Console#
```

IGMP Query Commands (Layer 2)

Command	Function	Mode	Page
ip igmp snooping querier	Allows this device to act as the querier for IGMP snooping	GC	4-201
ip igmp snooping query-count	Configures the query count	GC	4-202
ip igmp snooping query-interval	Configures the query interval	GC	4-203
ip igmp snooping query-max-response-time	Configures the report delay	GC	4-203
ip igmp snooping router-port-expire-time	Configures the query timeout	GC	4-204

ip igmp snooping querier

Use this command to enable the switch as an IGMP querier. Use the **no** form to disable it.

Syntax

```
ip igmp snooping querier
no ip igmp snooping querier
```

Default Setting

Enabled

Command Mode

Global Configuration

Command Usage

If enabled, the switch will serve as querier if elected. The querier is responsible for asking hosts if they want to receive multicast traffic.

Example

```
Console(config)#ip igmp snooping querier
Console(config)#
```

ip igmp snooping query-count

Use this command to configure the query count. Use the **no** form to restore the default.

Syntax

ip igmp snooping query-count *count*

no ip igmp snooping query-count

count - The maximum number of queries issued for which there has been no response before the switch takes action to drop a client from the multicast group. (Range: 2-10)

Default Setting

2 times

Command Mode

Global Configuration

Command Usage

The query count defines how long the querier waits for a response from a multicast client before taking action. If a querier has sent a number of queries defined by this command, but a client has not responded, a countdown timer is started using the time defined by **ip igmp snooping query-max- response-time**. If the countdown finishes, and the client still has not responded, then that client is considered to have left the multicast group.

Example

The following shows how to configure the query count to 10:

```
Console(config)#ip igmp snooping query-count 10
Console(config)#
```

Related Commands

ip igmp snooping query-max-response-time (4-203)

ip igmp snooping query-interval

Use this command to configure the query interval. Use the **no** form to restore the default.

Syntax

ip igmp snooping query-interval *seconds*

no ip igmp snooping query-interval

seconds - The frequency at which the switch sends IGMP host-query messages. (Range: 60-125)

Default Setting

125 seconds

Command Mode

Global Configuration

Example

The following shows how to configure the query interval to 100 seconds:

```
Console(config)#ip igmp snooping query-interval 100
Console(config)#
```

ip igmp snooping query-max-response-time

Use this command to configure the query report delay. Use the **no** form of this command to restore the default.

Syntax

ip igmp snooping query-max-response-time *seconds*

no ip igmp snooping query-max-response-time

seconds - The report delay advertised in IGMP queries. (Range: 5-30)

Default Setting

10 seconds

Command Mode

Global Configuration

Command Usage

- The switch must be using IGMPv2 for this command to take effect.
- This command defines the time after a query, during which a response is expected from a multicast client. If a querier has sent a number of queries defined by the **ip igmp snooping query-count**, but a client has not responded, a countdown timer is started using an initial value set by this command. If the countdown finishes, and the client still has not responded, then that client is considered to have left the multicast group.

Example

The following shows how to configure the maximum response time to 20 seconds:

```
Console(config)#ip igmp snooping query-max-response-time 20
Console(config)#
```

Related Commands

- ip igmp snooping version (4-198)
- ip igmp snooping query-max-response-time (4-203)

ip igmp snooping router-port-expire-time

Use this command to configure the query timeout. Use the **no** form of this command to restore the default.

Syntax

ip igmp snooping router-port-expire-time *seconds*

no ip igmp snooping router-port-expire-time

seconds - The time the switch waits after the previous querier stops before it considers the router port (i.e., the interface which had been receiving query packets) to have expired.
(Range: 300-500)

Default Setting

300 seconds

Command Mode

Global Configuration

Command Usage

The switch must use IGMPv2 for this command to take effect.

Example

The following shows how to configure the default timeout to 300 seconds:

```
Console(config)#ip igmp snooping router-port-expire-time 300
Console(config)#
```

Related Commands

ip igmp snooping version (4-198)

IGMP Commands (Layer 3)

Command	Function	Mode	Page
ip igmp	Enables IGMP for the specified interface	IC	4-206
ip igmp robustval	Configures the expected packet loss	IC	4-207
ip igmp query-interval	Configures frequency for sending host query messages	IC	4-207
ip igmp max-resp-interval	Configures the maximum host response time	IC	4-208
ip igmp last-memb-query-interval	Configures frequency for sending group-specific host query messages	IC	4-209
ip igmp version	Configures IGMP version used on this interface	IC	4-210
show ip igmp interface	Displays the IGMP configuration for specified interfaces	NE, PE	4-211
clear ip igmp group	Deletes entries from the IGMP cache	PE	4-212
show ip igmp groups	Displays detailed information for IGMP groups	NE, PE	4-213

ip igmp

Use this command to enable IGMP on a VLAN interface. Use the **no** form of this command to disable IGMP on the specified interface.

Syntax

ip igmp
no ip igmp

Default Setting

Disabled

Command Mode

Interface Configuration (VLAN)

Command Usage

IGMP query can be enabled globally at Layer 2 via the **ip igmp snooping** command, or enabled for specific VLAN interfaces at Layer 3 via the **ip igmp** command. (Layer 2 query is disabled if Layer 3 query is enabled.)

Example

```
Console(config)#interface vlan 1
Console(config-if)#ip igmp
Console(config-if)#end
Console#show ip igmp interface
Vlan 1 is up
  IGMP is enable, version is 2
  Robustness variable is 2
  Query interval is 125 sec
  Query Max Response Time is 10 sec,
  Last Member Query Interval is 1 sec
  Querier is 10.1.0.253
Console#
```

Related Commands

ip igmp snooping (4-197)
show ip igmp snooping (4-199)

ip igmp robustval

Use this command to specify the robustness (i.e., expected packet loss) for this interface. Use the **no** form of this command to restore the default value.

Syntax

ip igmp robustval *robust-value*

no ip igmp robustval

robust-value - The robustness of this interface. (Range: 1-255)

Default Setting

2

Command Mode

Interface Configuration (VLAN)

Command Usage

The robustness value is used in calculating the appropriate range for other IGMP variables, such as the Group Membership Interval (**ip igmp last-memb-query-interval**, page 4-209), as well as the Other Querier Present Interval, and the Startup Query Count (RFC 2236).

Example

```
Console(config-if)#ip igmp robustval 3
Console(config-if)#
```

ip igmp query-interval

Use this command to configure the frequency at which host query messages are sent. Use the **no** form to restore the default.

Syntax

ip igmp query-interval *seconds*

no ip igmp query-interval

seconds - The frequency at which the switch sends IGMP host-query messages. (Range: 1-255)

Default Setting

125 seconds

Command Mode

Interface Configuration (VLAN)

Command Usage

- Multicast routers send host query messages to determine the interfaces that are connected to downstream hosts requesting a specific multicast service. Only the designated multicast router for a subnet sends host query messages, which are addressed to the multicast address 224.0.0.1.
- For IGMP Version 1, the designated router is elected according to the multicast routing protocol that runs on the LAN. But for IGMP Version 2, the designated querier is the lowest IP-addressed multicast router on the subnet.

Example

The following shows how to configure the query interval to 100 seconds:

```
Console(config-if)#ip igmp query-interval 100
Console(config-if)#
```

ip igmp max-resp-interval

Use this command to configure the maximum response time advertised in IGMP queries. Use the **no** form of this command to restore the default.

Syntax

ip igmp max-resp-interval *seconds*

no ip igmp max-resp-interval

seconds - The report delay advertised in IGMP queries.

(Range: 1-255)

Default Setting

10 seconds

Command Mode

Interface Configuration (VLAN)

Command Usage

- The switch must be using IGMPv2 for this command to take effect.
- This command defines how long any responder (i.e., client or router) still in the group has to respond to a query message before the router deletes the group.
- By varying the Maximum Response Interval, you can tune the burstiness of IGMP messages passed on the subnet; where larger values make the traffic less bursty, as host responses are spread out over a larger interval.
- The number of seconds represented by the maximum response interval must be less than the Query Interval (page 4-207).

Example

The following shows how to configure the maximum response time to 20 seconds:

```
Console(config-if)#ip igmp max-resp-interval 20
Console(config-if)#
```

Related Commands

ip igmp version (4-210)
ip igmp query-interval (4-207)

ip igmp last-memb-query-interval

Use this command to configure the last member query interval. Use the **no** form of this command to restore the default.

Syntax

ip igmp last-memb-query-interval *seconds*

no ip igmp last-memb-query-interval

seconds - The report delay for the last member query. (Range: 1-255)

Default Setting

1 second

Command Mode

Interface Configuration (VLAN)

Command Usage

- A multicast client sends an IGMP leave message when it leaves a group. The router then checks to see if this was the last host in the group by sending an IGMP query and starting a timer based on this command. If no reports are received before the timer expires, the group is deleted.
- This value may be tuned to modify the leave latency of the network. A reduced value results in reduced time to detect the loss of the last member of a group.

Example

The following shows how to configure the maximum response time to 10 seconds:

```
Console(config-if)#ip igmp last-memb-query-interval 10
Console(config-if)#
```

ip igmp version

Use this command to configure the IGMP version used on an interface. Use the **no** form of this command to restore the default.

Syntax

ip igmp version {1 | 2}
no ip igmp version

- 1 - IGMP Version 1
- 2 - IGMP Version 2

Default Setting

IGMP Version 2

Command Mode

Interface Configuration (VLAN)

Command Usage

- All routers on the subnet must support the same version. However, the multicast hosts on the subnet may support either IGMP version 1 or 2.
- The switch must be set to version 2 to enable the **ip igmp max-resp-interval** (page 4-208).

Example

The following configures the switch to use IGMP Version 1 on the selected interface:

```
Console(config-if)#ip igmp version 1
Console(config-if)#
```

show ip igmp interface

Use this command to show the IGMP configuration for a specific VLAN interface or for all interfaces.

Syntax

show ip igmp interface [vlan *vlan-id*]
vlan-id - VLAN ID (Range: 1-4094)

Default Setting

None

Command Mode

Normal Exec, Privileged Exec

Example

The following example shows the IGMP configuration for VLAN 1, as well as the device currently serving as the IGMP querier for this multicast service.

```
Console#show ip igmp interface vlan 1
Vlan 1 is up
  IGMP is enable, version is 2
  Robustness variable is 2
  Query interval is 125 sec
  Query Max Response Time is 10 sec,
  Last Member Query Interval is 1 sec
  Querier is 10.1.0.253
Console#
```

clear ip igmp group

Use this command to delete entries from the IGMP cache.

Syntax

clear ip igmp group [*group-address* | **interface vlan** *vlan-id*]

- *group-address* - IP address of the multicast group.
- *vlan-id* - VLAN ID (Range: 1-4094)

Default Setting

Deletes all entries in the cache if no options are selected.

Command Mode

Privileged Exec

Command Usage

Enter the address for a multicast group to delete all entries for the specified group. Enter the interface option to delete all multicast groups for the specified interface. Enter no options to clear all multicast groups from the cache.

Example

The following example clears all multicast group entries for VLAN 1:

```
Console#clear ip igmp group interface vlan 1
Console#
```

show ip igmp groups

Use this command to display information on multicast groups active on this switch.

Syntax

show ip igmp groups [*group-address* | **interface vlan** *vlan-id*]

- *group-address* - IP address of the multicast group.
- *vlan-id* - VLAN ID (Range: 1-4094)

Default Setting

Displays information for all known groups.

Command Mode

Normal Exec, Privileged Exec

Command Usage

- This command displays information for multicast groups learned via IGMP, not static groups.
- If the switch receives an IGMP Version 1 Membership Report, it sets a timer to note that there are Version 1 hosts present which are members of the group for which it heard the report.
- If there are Version 1 hosts present for a particular group, the switch will ignore any Leave Group messages that it receives for that group.

Example

The following shows the IGMP groups currently active on VLAN 1:

Console#show ip igmp groups vlan 1					
GroupAddress	InterfaceVlan	Lastreporter	Uptime	Expire	VlTimer
234.5.6.8	1	10.1.5.19	7068	220	0
Console#					

Field	Description
GroupAddress	IP multicast group address with subscribers directly attached or downstream from this switch.
InterfaceVlan	The interface on this switch that has received traffic directed to the multicast group address.
Lastreporter	The IP address of the source of the last membership report received for this multicast group address on this interface. If no membership report has been received, this object has the value 0.0.0.0.
Uptime	The time elapsed since this entry was created.
Expire	The time remaining before this entry will be aged out. (The default is 260 seconds.)
VlTimer	The time remaining until the switch assumes that there are no longer any IGMP Version 1 members on the IP subnet attached to this interface. (The default is 400 seconds.)

IP Interface Commands

There are no IP addresses assigned to this router by default. You must manually configure a new address to manage the router over your network or to connect the router to existing IP subnets. You may also need to establish a default gateway between this device and management stations or other devices that exist on another network segment (if routing is not enabled).

This section includes commands for configuring IP interfaces, the Address Resolution Protocol (ARP) and Proxy ARP. These commands are used to connect subnetworks to the enterprise network.

Command Group	Function	Page
Basic IP Configuration	Configures the IP address for interfaces and the gateway router	4-215
Address Resolution Protocol (ARP)	Configures static, dynamic and proxy ARP service	4-221

Basic IP Configuration

Command	Function	Mode	Page
ip address	Sets the IP address for the current interface	IC	4-216
ip default-gateway	Defines the default gateway through which this router can reach other subnetworks	GC	4-218
show ip interface	Displays the IP settings for this device	PE	4-219
show ip redirects	Displays the default gateway configured for this device	PE	4-219
ping	Sends ICMP echo request packets to another node on the network	NE, PE	4-220

ip address

Use this command to set the IP address for the currently selected VLAN interface. Use the **no** form to restore the default IP address.

Syntax

ip address {*ip-address netmask* | **bootp** | **dhcp**} [*secondary*]

no ip address

- *ip-address* - IP address
- *netmask* - Network mask for the associated IP subnet. This mask identifies the host address bits used for routing to specific subnets.
- **bootp** - Obtains IP address from BOOTP.
- **dhcp** - Obtains IP address from DHCP.
- *secondary* - Specifies a secondary IP address.

Default Setting

IP address: 0.0.0.0

Netmask: 255.0.0.0

Command Mode

Interface Configuration (VLAN)

Command Usage

- If this router is directly connected to end node devices (or connected to end nodes via shared media) that will be assigned to a specific subnet, then you must create a router interface for each VLAN that will support routing. The router interface consists of an IP address and subnet mask. This interface address defines both the network number to which the router interface is attached and the router's host number on that network. In other words, a router interface address defines the network and subnetwork numbers of the segment that is connected to that interface, and allows you to send IP packets to or from the router.
- Before you configure any network interfaces on this router, you should first create a VLAN for each unique user group, or for each network application and its associated users. Then assign the ports associated with each of these VLANs.
- You must assign an IP address to this device to gain management access over the network or to connect the router to existing IP subnets.

You can manually configure a specific IP address, or direct the device to obtain an address from a BOOTP or DHCP server. Valid IP addresses consist of four numbers, 0 to 255, separated by periods. Anything outside this format will not be accepted by the configuration program.

- An interface can have only one primary IP address, but can have many secondary IP addresses. In other words, you will need to specify secondary addresses if more than one IP subnet can be accessed via this interface.
- If you select the **bootp** or **dhcp** option, IP is enabled but will not function until a BOOTP or DHCP reply has been received. Requests will be broadcast periodically by this device in an effort to learn its IP address. (BOOTP and DHCP values can include the IP address, default gateway, and subnet mask).
- You can start broadcasting BOOTP or DHCP requests by entering an **ip dhcp restart client** command, or by rebooting the router.

- Notes:**
1. Each VLAN group can be assigned its own IP interface address. Therefore, if routing is enabled, you can manage the router via any of these IP addresses.
 2. Before you can change the primary IP address on an interface, you must first clear the current address with the **no** form of this command.

Example

In the following example, the device is assigned an address in VLAN 1.

```
Console(config)#interface vlan 1
Console(config-if)#ip address 192.168.1.5 255.255.255.0
Console(config-if)#
```

Related Commands

ip dhcp restart client (4-98)

ip default-gateway

Use this command to establish a static route between this router and devices that exist on another network segment. Use the **no** form to remove the static route.

Syntax

ip default-gateway *gateway*

no ip default-gateway

gateway - IP address of the default gateway

Default Setting

No static route is established.

Command Mode

Global Configuration

Command Usage

- The gateway specified in this command is only valid if routing is disabled with the **no ip routing** command. If IP routing is disabled, you must define a gateway if the target device is located in a different subnet.
- If routing is enabled, you must define the gateway with the **ip route** command.

Example

The following example defines a default gateway for this device:

```
Console(config)#ip default-gateway 10.1.1.254
Console(config)#
```

Related Commands

show ip redirects (4-219)

ip routing (4-226)

ip route (4-227)

show ip interface

Use this command to display the settings of an IP interface.

Default Setting

All interfaces

Command Mode

Privileged Exec

Example

```
Console#show ip interface
Vlan 1 is up, addressing mode is User
  Interface address is 10.1.0.254, mask is 255.255.255.0, Primary
  MTU is 1500 bytes
  Proxy ARP is disabled
  Split horizon is enabled
Console#
```

Related Commands

show ip redirects (4-219)

show ip redirects

Use this command to show the default gateway configured for this device.

Default Setting

None

Command Mode

Privileged Exec

Example

```
Console#show ip redirects
ip default gateway 10.1.0.254
Console#
```

Related Commands

ip default-gateway (4-218)

ping

Use this command to send ICMP echo request packets to another node on the network.

Syntax

ping *host* [**count** *count*][**size** *size*]

- *host* - IP address or IP alias of the host.
- *count* - Number of packets to send. (Range: 1-16, default: 5)
- *size* - Number of bytes in a packet. (Range: 32-512, default: 32)
The actual packet size will be eight bytes larger than the size specified because the router adds header information.

Default Setting

This command has no default for the host.

Command Mode

Normal Exec, Privileged Exec

Command Usage

- Use the ping command to see if another site on the network can be reached.
- Following are some results of the **ping** command:
 - *Normal response* - The normal response occurs in one to ten seconds, depending on network traffic.
 - *Destination does not respond* - If the host does not respond, a “timeout” appears in ten seconds.
 - *Destination unreachable* - The gateway for this destination indicates that the destination is unreachable.
 - *Network or host unreachable* - The gateway found no corresponding entry in the route table.
- Press <Esc> to stop pinging.

Example

```

Console#ping 10.1.0.9
Type ESC to abort.
PING to 10.1.0.9, by 5 32-byte payload ICMP packets,
  timeout is 5 seconds
response time: 10 ms
response time: 10 ms
response time: 10 ms
response time: 10 ms
response time: 0 ms
Ping statistics for 10.1.0.9:
  5 packets transmitted, 5 packets received (100%),
  0 packets lost (0%)
Approximate round trip times:
  Minimum = 0 ms, Maximum = 10 ms, Average = 8 ms
Console#

```

Related Commands

interface (4-119)

Address Resolution Protocol (ARP)

Command	Function	Mode	Page
arp	Adds a static entry in the ARP cache	GC	4-222
arp-timeout	Sets the time a dynamic entry remains in the ARP cache	GC	4-223
clear arp-cache	Deletes all dynamic entries from the ARP cache	PE	4-223
show arp	Displays entries in the ARP cache	NE, PE	4-224
ip proxy-arp	Enables proxy ARP service	VC	4-224

arp

Use this command to add a static entry in the Address Resolution Protocol (ARP) cache. Use the **no** form to remove an entry from the cache.

Syntax

arp *ip-address hardware-address*

no arp *ip-address*

- *ip-address* - IP address to map to a specified hardware address.
- *hardware-address* - Hardware address to map to a specified IP address.
(The format for this address is xx-xx-xx-xx-xx-xx.)

Default Setting

No default entries

Command Mode

Global Configuration

Command Usage

- The ARP cache is used to map 32-bit IP addresses into 48-bit hardware (i.e., Media Access Control) addresses. This cache includes entries for hosts and other routers on local network interfaces defined on this router.
- The maximum number of static entries allowed in the ARP cache is 128.
- You may need to enter a static entry in the cache if there is no response to an ARP broadcast message. For example, some applications may not respond to ARP requests or the response arrives too late, causing network operations to time out.

Example

```
Console(config)#arp 10.1.0.19 01-02-03-04-05-06
Console(config)#
```

Related Commands

clear arp-cache
show arp

arp-timeout

Use this command to set the aging time for dynamic entries in the Address Resolution Protocol (ARP) cache. Use the **no** form to restore the default.

Syntax

arp-timeout *seconds*

no arp-timeout

seconds - The time a dynamic entry remains in the ARP cache.
(Range: 300-86400; 86400 is one day)

Default Setting

1200 seconds (20 minutes)

Command Mode

Global Configuration

Command Usage

Use the **show arp** command to display the current cache timeout value.

Example

This example sets the ARP cache timeout for 15 minutes (i.e., 900 seconds).

```
Console(config)#arp-timeout 900
Console(config)#
```

clear arp-cache

Use this command to delete all dynamic entries from the Address Resolution Protocol (ARP) cache.

Command Mode

Privileged Exec

Example

This example clears all dynamic entries in the ARP cache.

```
Console#clear arp-cache
This operation will delete all the dynamic entries in ARP Cache.
Are you sure to continue this operation (y/n)?y
Console#
```

show arp

Use this command to display entries in the Address Resolution Protocol (ARP) cache.

Command Mode

Normal Exec, Privileged Exec

Command Usage

This command displays information about the ARP cache. The first line shows the cache timeout. It also shows each cache entry, including the corresponding IP address, MAC address, type (static, dynamic, other), and VLAN interface. Note that entry type “other” indicates local addresses for this router.

Example

This example displays all entries in the ARP cache.

```
Console#show arp
Arp cache timeout: 1200 (seconds)

  IP Address      MAC Address      Type      Interface
-----
    10.1.0.0  ff-ff-ff-ff-ff-ff  other          1
    10.1.0.254  00-00-ab-cd-00-00  other          1
    10.1.0.255  ff-ff-ff-ff-ff-ff  other          1
  123.20.10.123  02-10-20-30-40-50  static         2
    345.30.20.23  09-50-40-30-20-10  dynamic        3

Total entry : 5
Console#
```

ip proxy-arp

Use this command to enable proxy Address Resolution Protocol (ARP).
Use the **no** form to disable proxy ARP.

Syntax

- ip proxy-arp**
- no ip proxy-arp**

Default Setting

Disabled

Command Mode

Interface Configuration (VLAN)

Command Usage

Proxy ARP allows a non-routing device to determine the MAC address of a host on another subnet or network.

Example

```
Console(config)#interface vlan 3
Console(config-if)#ip proxy-arp
Console(config-if)#
```

IP Routing Commands

After you configure network interfaces for this router, you must set the paths used to send traffic between different interfaces. If you enable routing on this device, traffic will automatically be forwarded between all of the local subnetworks. However, to forward traffic to devices on other subnetworks, you can either configure fixed paths with static routing commands, or enable a dynamic routing protocol that exchanges information with other routers on the network to automatically determine the best path to any subnetwork.

This section includes commands for both static and dynamic routing. These commands are used to connect between different local subnetworks or to connect the router to the enterprise network.

Command Group	Function	Page
Global Routing Configuration	Configures global parameters for static and dynamic routing, displays the routing table, and statistics for protocols used to exchange routing information	4-226
Routing Information Protocol (RIP)	Configures global and interface specific parameters for RIP	4-231
Open Shortest Path First (OSPF)	Configures global and interface specific parameters for OSPF	4-244

Global Routing Configuration

Command	Function	Mode	Page
ip routing	Enables static and dynamic IP routing	GC	4-226
ip route	Configures static routes	GC	4-227
clear ip route	Deletes specified entries from the routing table	PE	4-228
show ip route	Displays specified entries in the routing table	PE	4-228
show ip traffic	Displays statistics for IP, ICMP, UDP, TCP and ARP protocols	PE	4-229

ip routing

Use this command to enable IP routing. Use the **no** form to disable IP routing.

Syntax

ip routing
no ip routing

Default Setting

Enabled

Command Mode

Global Configuration

Command Usage

- The command affects both static and dynamic unicast routing.
- If IP routing is enabled, all IP packets are routed using either static routing or dynamic routing via RIP or OSPF, and other packets for all non-IP protocols (e.g., NetBuei, NetWare or AppleTalk) are switched based on MAC addresses. If IP routing is disabled, all packets are switched, with filtering and forwarding decisions based strictly on MAC addresses.

Example

```
Console(config)#ip routing
Console(config)#
```


ip route

Use this command to configure static routes. Use the **no** form to remove static routes.

Syntax

ip route {*destination-ip* *netmask* | **default**} {*gateway*} [**metric** *metric*]
no ip route {*destination-ip* *netmask* | **default** | *}

- *destination-ip* – IP address of the destination network, subnetwork, or host.
- *netmask* – Network mask for the associated IP subnet. This mask identifies the host address bits used for routing to specific subnets.
- **default** – Sets this entry as the default route.
- *gateway* – IP address of the gateway used for this route.
- *metric* – Selected RIP cost for this interface. (Range: 1-5, default: 1)
- * – Removes all static routing table entries.

Default Setting

No static routes are configured.

Command Mode

Global Configuration

Command Usage

- You can configure up to 2000 static routes.
- Static routes take precedence over dynamically learned routes.
- Static routes are included in RIP updates periodically sent by the router.

Example

This example forwards all traffic for subnet 192.168.1.0 to the router 192.168.5.254, using the default metric of 1.

```
Console(config)#ip route 192.168.1.0 255.255.255.0 192.168.5.254
Console(config)#
```

clear ip route

Use this command to remove dynamically learned entries from the IP routing table.

Syntax

clear ip route {*network* [*netmask*] | *}}

- *network* – Network or subnet address.
- *netmask* - Network mask for the associated IP subnet. This mask identifies the host address bits used for routing to specific subnets.
- * – Removes all dynamic routing table entries.

Command Mode

Privileged Exec

Command Usage

- This command only clears dynamically learned routes.
- Use the **no ip address** command to remove a local interface.
- Use the **no ip route** command to remove a static route.

Example

```
Console#clear ip route 10.1.5.0
Console#
```

show ip route

Use this command to display information in the IP routing table.

Syntax

show ip route [*config* | *address* [*netmask*]]

- **config** – Displays all static routing entries.
- *address* – IP address of the destination network, subnetwork or host for which routing information is to be displayed.
- *netmask* - Network mask for the associated IP subnet. This mask identifies the host address bits used for routing to specific subnets.

Command Mode

Privileged Exec

Command Usage

If the *address* is specified without the *netmask* parameter, the router displays all routes for the corresponding natural class address (page 4-233).

Example

Console#show ip route						
Ip Address	Netmask	Next Hop	Protocol	Metric	Interface	
0.0.0.0	0.0.0.0	10.2.48.102	static	0	1	
10.2.48.2	255.255.252.0	10.2.48.16	local	0	1	
10.2.5.6	255.255.255.0	10.2.8.12	RIP	1	2	
10.3.9.1	255.255.255.0	10.2.9.254	OSPF-intra	2	3	
Total entry: 4						
Console#						

Field	Description
Ip Address	IP address of the destination network, subnetwork, or host. Note that the address 0.0.0.0 indicates the default gateway for this router.
Netmask	Network mask for the associated IP subnet.
Next Hop	IP address of the next hop (or gateway) used for this route.
Protocol	The protocol which generated this route information. (Values: static, local, RIP, OSPF)
Metric	Cost for this interface.
Interface	VLAN interface through which this address can be reached.

show ip traffic

Use this command to display statistics for IP, ICMP, UDP, TCP and ARP protocols.

Command Mode

Privileged Exec

Command Usage

For a description of the information shown by this command, see “Displaying Statistics for IP Protocols” on page 3-165.

Example

```
Console#show ip traffic
IP statistics:
  Rcvd: 5 total, 5 local destination
        0 checksum errors
        0 unknown protocol, 0 not a gateway
  Frags: 0 reassembled, 0 timeouts
        0 fragmented, 0 couldn't fragment
  Sent: 9 generated
        0 no route
ICMP statistics:
  Rcvd: 0 checksum errors, 0 redirects, 0 unreachable, 0 echo
        5 echo reply, 0 mask requests, 0 mask replies, 0 quench
        0 parameter, 0 timestamp
  Sent: 0 redirects, 0 unreachable, 0 echo, 0 echo reply
        0 mask requests, 0 mask replies, 0 quench, 0 timestamp
        0 time exceeded, 0 parameter problem
UDP statistics:
  Rcvd: 0 total, 0 checksum errors, 0 no port
  Sent: 0 total
TCP statistics:
  Rcvd: 0 total, 0 checksum errors
  Sent: 0 total
ARP statistics:
  Rcvd: 0 requests, 1 replies
  Sent: 1 requests, 0 replies
Console#
```

Routing Information Protocol (RIP)

Command	Function	Mode	Page
router rip	Enables the RIP routing protocol	GC	4-231
timers basic	Sets basic timers, including update, timeout, garbage collection	RC	4-232
network	Specifies the network interfaces that are to use RIP routing	RC	4-233
neighbor	Defines a neighboring router with which to exchange information	RC	4-234
version	Specifies the RIP version to use on all network interfaces (if not already specified with a receive version or send version command)	RC	4-235
ip rip receive version	Sets the RIP receive version to use on a network interface	IC	4-236
ip rip send version	Sets the RIP send version to use on a network interface	IC	4-237
ip split-horizon	Enables split-horizon or poison-reverse loop prevention	IC	4-239
ip rip authentication key	Enables authentication for RIP2 packets and specifies keys	IC	4-240
ip rip authentication mode	Specifies the type of authentication used for RIP2 packets	IC	4-241
show rip globals	Displays global configuration settings and statistics for RIP	PE	4-242
show ip rip	Displays RIP configuration information for each network interface	PE	4-242

router rip

Use this command to enable Routing Information Protocol (RIP) routing for all IP interfaces on the router. Use the **no** form to disable it.

Syntax

router rip

no router rip

Command Mode

Global Configuration

Default Setting

Disabled

Command Usage

- RIP is used to specify how routers exchange routing table information.
- This command is also used to enter router configuration mode.

Example

```
Console(config)#router rip
Console(config-router)#
```

Related Commands

network (4-233)

timers basic

Use this command to configure the RIP update timer, timeout timer, and garbage- collection timer. Use the **no** form to restore the defaults.

Syntax

timers basic *update-seconds*

no timers basic

update-seconds – Sets the update timer to the specified value, sets the timeout time value to 6 times the update time, and sets the garbage- collection timer to 4 times the update time.
(Range for update timer: 15-60 seconds)

Command Mode

Router Configuration

Default Setting

Update: 30 seconds

Timeout: 180 seconds

Garbage collection: 120 seconds

Command Usage

- The *update* timer sets the rate at which updates are sent. This is the fundamental timer used to control all basic RIP processes.
- The *timeout* timer is the time after which there have been no update messages that a route is declared dead. The route is marked inaccessible (i.e., the metric set to infinite) and advertised as unreachable. However, packets are still forwarded on this route.
- After the *timeout* interval expires, the router waits for an interval specified by the *garbage-collection* timer before removing this entry from the routing table. This timer allows neighbors to become aware of an invalid route prior to purging it.
- Setting the update timer to a short interval can cause the router to spend an excessive amount of time processing updates.
- These timers must be set to the same values for all routers in the network.

Example

This example sets the update timer to 40 seconds. The timeout timer is subsequently set to 240 seconds, and the garbage-collection timer to 160 seconds.

```
Console(config-router)#timers basic 15
Console(config-router)#
```

network

Use this command to specify the network interfaces that will be included in the RIP routing process. Use the **no** form to remove an entry.

Syntax

network *subnet-address*

no network *subnet-address*

subnet-address – IP address of a network directly connected to this router.

Command Mode

Router Configuration

Default Setting

No networks are specified.

Command Usage

- RIP only sends updates to interfaces specified by this command.
- Subnet addresses are interpreted as class A, B or C, based on the first field in the specified address. In other words, if a subnet address `nnn.xxx.xxx.xxx` is entered, the first field (`nnn`) determines the class:
 - 0 - 127 is class A, and only the first field in the network address is used.
 - 128 - 191 is class B, and the first two fields in the network address are used.
 - 192 - 223 is class C, and the first three fields in the network address are used.

Example

This example includes network interface 10.1.0.0 in the RIP routing process.

```
Console(config-router)#network 10.1.0.0
Console(config-router)#
```

Related Commands

`router rip` (4-231)

neighbor

Use this command to define a neighboring router with which this router will exchange routing information. Use the **no** form to remove an entry.

Syntax

neighbor *ip-address*

no neighbor *ip-address*

ip-address - IP address to map to a specified hardware address.

Command Mode

Router Configuration

Default Setting

No neighbors are defined.

Command Usage

This command can be used to configure a static neighbor with which this router will exchange information, rather than relying on broadcast messages generated by the RIP protocol.

Example

```
Console(config-router)#neighbor 10.2.0.254
Console(config-router)#
```

version

Use this command to specify a RIP version used globally by the router. Use the **no** form to restore the default value.

Syntax

version {1 | 2}

no version

- **1** - RIP Version 1
- **2** - RIP Version 2

Command Mode

Router Configuration

Default Setting

RIP Version 1

Command Usage

- When this command is used to specify a global RIP version, any VLAN interface not previously set by the **ip rip receive version** or **ip rip send version** command will be set to the following values:
 - RIP Version 1 configures the unset interfaces to send RIPv1 compatible protocol messages and receive either RIPv1 or RIPv2 protocol messages.
 - RIP Version 2 configures the unset interfaces to use RIPv2 for both sending and receiving protocol messages.
- When the **no** form of this command is used to restore the default value, any VLAN interface not previously set by the **ip rip receive version** or **ip rip send version** command will be set to the default send or receive version.

Example

This example sets the global version for RIP to send and receive version 2 packets.

```
Console(config-router)#version 2
Console(config-router)#
```

Related Commands

ip rip receive version (4-236)
ip rip send version (4-237)

ip rip receive version

Use this command to specify a RIP version to receive on an interface. Use the **no** form to restore the default value.

Syntax

ip rip receive version {none | 1 | 2 | 1 2}
no ip rip receive version

- **none** - Does not accept incoming RIP packets.
- **1** - Accepts only RIPv1 packets.
- **2** - Accepts only RIPv2 packets.
- **1 2** - Accepts RIPv1 or RIPv2 packets

Command Mode

Interface Configuration (VLAN)

Default Setting

The default depends on the setting specified with the **version** command:

Global RIPv1 - RIPv1 or RIPv2 packets
Global RIPv2 - RIPv2 packets

Command Usage

- Use this command to override the global setting specified by the RIP **version** command.

- You can specify the receive version based on these options:
 - Use “none” if you do not want to add any dynamic entries to the routing table for an interface. (For example, you may only want to allow static routes for a specific interface.)
 - Use “1” or “2” if all routers in the local network are based on RIPv1 or RIPv2, respectively.
 - Use “1 2” if some routers in the local network are using RIPv2, but there are still some older routers using RIPv1.

Example

This example sets the interface version for VLAN 1 to receive RIPv1 packets.

```
Console(config)#interface vlan 1
Console(config-if)#ip rip receive version 1
Console(config-if)#
```

Related Commands

version (4-235)

ip rip send version

Use this command to specify a RIP version to send on an interface. Use the **no** form to restore the default value.

Syntax

ip rip send version {none | 1 | 2 | v2-broadcast}
no ip rip send version

- **none** - Does not transmit RIP updates.
- **1** - Sends only RIPv1 packets.
- **2** - Sends only RIPv2 packets.
- **v2-broadcast** - Route information is broadcast to other routers with RIPv2.

Command Mode

Interface Configuration (VLAN)

Default Setting

The default depends on the setting specified with the **version** command:

Global RIPv1 - Routes broadcast to other routers with RIPv2

Global RIPv2 - RIPv2 packets

Command Usage

- Use this command to override the global setting specified by the **RIP version** command.
- You can specify the receive version based on these options:
 - Use “none” to passively monitor route information advertised by other routers attached to the network.
 - Use “1” or “2” if all routers in the local network are based on RIPv1 or RIPv2, respectively.
 - Use “v2-broadcast” to propagate route information by broadcasting to other routers on the network using RIPv2, instead of multicasting as normally required by RIPv2. (Using this mode allows RIPv1 routers to receive these protocol messages, but still allows RIPv2 routers to receive the additional information provided by RIPv2, including subnet mask, next hop and authentication information.)

Example

This example sets the interface version for VLAN 1 to send RIPv1 packets.

```
Console(config)#interface vlan 1
Console(config-if)#ip rip send version 1
Console(config-if)#
```

Related Commands

version (4-235)

ip split-horizon

Use this command to enable split-horizon or poison-reverse (a variation) on an interface. Use the **no** form to disable split-horizon.

Syntax

ip split-horizon [poison-reverse]

no ip split-horizon

poison-reverse - Enables poison-reverse on the current interface.

Command Mode

Interface Configuration (VLAN)

Default Setting

split-horizon

Command Usage

- Split horizon never propagates routes back to an interface from which they have been acquired.
- Poison reverse propagates routes back to an interface port from which they have been acquired, but sets the distance-vector metrics to infinity. (This provides faster convergence.)

Example

This example propagates routes back to the source using poison-reverse.

```
Console(config)#interface vlan 1
Console(config-if)#ip split-horizon poison-reverse
Console(config-if)#
```

ip rip authentication key

Use this command to enable authentication for RIPv2 packets and to specify the key that must be used on an interface. Use the **no** form to prevent authentication.

Syntax

ip rip authentication key *key-string*

no ip rip authentication

key-string - A password used for authentication.

(Range: 1-16 characters, case sensitive)

Command Mode

Interface Configuration (VLAN)

Default Setting

No authentication

Command Usage

- This command can be used to restrict the interfaces that can exchange RIPv2 routing information. (Note that this command does not apply to RIPv1.)
- For authentication to function properly, both the sending and receiving interface must be configured with the same password.

Example

This example sets an authentication password of “small” to verify incoming routing messages and to tag outgoing routing messages.

```
Console(config)#interface vlan 1
Console(config-if)#ip rip authentication key small
Console(config-if)#
```

Related Commands

ip rip authentication mode (4-241)

ip rip authentication mode

Use this command to specify the type of authentication that can be used on an interface. Note that the current firmware version only supports a simple password. Use the **no** form to restore the default value.

Syntax

ip rip authentication mode {text}

no ip rip authentication mode

text - Indicates that a simple password will be used.

Command Mode

Interface Configuration (VLAN)

Default Setting

No authentication

Command Usage

- The password to be used for authentication is specified in the **ip rip authentication key** command (page 4-240).
- This command requires the interface to exchange routing information with other routers based on an authorized password. (Note that this command only applies to RIPv2.)
- For authentication to function properly, both the sending and receiving interface must be configured with the same password or authentication key.

Example

This example sets the authentication mode to plain text.

```
Console(config)#interface vlan 1
Console(config-if)#ip rip authentication mode text
Console(config-if)#
```

Related Commands

ip rip authentication key (4-240)

show rip globals

Use this command to display global configuration settings for RIP.

Command Mode

Privileged Exec

Example

```
Console#show rip globals
RIP Process: Enabled
Update Time in Seconds: 30
Number of Route Change: 0
Number of Queries: 1
Console#
```

Field	Description
RIP Process	Indicates if RIP has been enabled or disabled.
Update Time in Seconds	The interval at which RIP advertises known route information. (Default: 30 seconds)
Number of Route Changes	Number of times routing information has changed.
Number of Queries	Number of router database queries received by this router.

show ip rip

Use this command to display information about interfaces configured for RIP.

Syntax

show ip rip {configuration | status | peer}

- **configuration** - Shows RIP configuration settings for each interface.
- **status** - Shows the status of routing messages on each interface.
- **peer** - Shows information on neighboring routers, along with information about the last time a route update was received, the RIP version used by the neighbor, and the status of routing messages received from this neighbor.

Command Mode

Privileged Exec

Example

```

Console#show ip rip configuration

```

Interface	SendMode	ReceiveMode	Poison	Authentication
10.1.0.253	rip1Compatible	RIPv1Orv2	SplitHorizon	noAuthentication
10.1.1.253	rip1Compatible	RIPv1Orv2	SplitHorizon	noAuthentication

```

Console#show ip rip status

```

Interface	RcvBadPackets	RcvBadRoutes	SendUpdates
10.1.0.253	0	0	13
10.1.1.253	0	0	13

```

Console#show ip rip peer

```

Peer	UpdateTime	Version	RcvBadPackets	RcvBadRoutes
10.1.0.254	1625	2	0	0
10.1.1.254	1625	2	0	0

```

Console#

```

Field	Description
<i>show ip rip configuration</i>	
Interface	IP address of the interface.
SendMode	RIP version sent on this interface (none, RIPv1, RIPv2, or RIPv2-broadcast)
ReceiveMode	RIP version received on this interface (none, RIPv1, RIPv2, RIPv1 or RIPv2)
Poison	Shows if split-horizon, poison-reverse, or no protocol message loopback prevention method is in use.
Authentication	Shows if authentication is set to simple password or none.
<i>show ip rip status</i>	
Interface	IP address of the interface.
RcvBadPackets	Number of bad RIP packets received.
RcvBadRoutes	Number of bad routes received.
SendUpdates	Number of route changes.
<i>show ip rip peer</i>	
Peer	IP address of a neighboring RIP router.
UpdateTime	Last time a route update was received from this peer.

Field	Description
Version	Whether RIPv1 or RIPv2 packets were received from this peer.
RcvBadPackets	Number of bad RIP packets received from this peer.
RcvBadRoutes	Number of bad routes received from this peer.

Open Shortest Path First (OSPF)

Command	Function	Mode	Page
<i>General Configuration</i>			
router ospf	Enables or disables OSPF	GC	4-246
router-id	Sets the router ID for this device	RC	4-247
compatible rfc1583	Calculates summary route costs using RFC 1583 (OSPFv1)	RC	4-248
default-information originate	Generates a default external route into an autonomous system	RC	4-248
timers spf	Configures the hold time between consecutive SPF calculations	RC	4-250
<i>Route Metrics and Summaries</i>			
area range	Summarizes routes advertised by an ABR	RC	4-251
area default-cost	Sets the cost for a default summary route sent into a stub or NSSA	RC	4-252
summary-address	Summarizes routes advertised by an ASBR	RC	4-253
redistribute	Redistribute routes from one routing domain to another	RC	4-254
<i>Area Configuration</i>			
network area	Assigns specified interface to an area	RC	4-255
area stub	Defines a stubby area that cannot send or receive LSAs	RC	4-257
area nssa	Defines a not-so-stubby that can import external routes	RC	4-258
area virtual-link	Defines a virtual link from an area border routers to the backbone	RC	4-260

Command	Function	Mode	Page
<i>Interface Configuration</i>			
ip ospf authentication	Specifies the authentication type for an interface	IC	4-263
ip ospf authentication-key	Assigns a simple password to be used by neighboring routers	IC	4-264
ip ospf message-digest-key	Enables MD5 authentication and sets the key for an interface	IC	4-265
ip ospf cost	Specifies the cost of sending a packet on an interface	IC	4-266
ip ospf dead-interval	Sets the interval at which hello packets are not seen before neighbors declare the router down	IC	4-267
ip ospf hello-interval	Specifies the interval between sending hello packets	IC	4-268
ip ospf priority	Sets the router priority used to determine the designated router	IC	4-268
ip ospf retransmit-interval	Specifies the time between resending a link-state advertisement	IC	4-269
ip ospf transmit-delay	Estimates time to send a link-state update packet over an interface	IC	4-270
<i>Display Information</i>			
show ip ospf	Displays general information about the routing processes	PE	4-271
show ip ospf border-routers	Displays routing table entries for Area Border Routers (ABR) and Autonomous System Boundary Routers (ASBR)	PE	4-272
show ip ospf database	Shows information about different LSAs in the database	PE	4-273
show ip ospf interface	Displays interface information	PE	4-281
show ip ospf neighbor	Displays neighbor information	PE	4-282

Command	Function	Mode	Page
show ip ospf summary-address	Displays all summary address redistribution information	PE	4-283
show ip ospf virtual-links	Displays parameters and the adjacency state of virtual links	PE	4-284

router ospf

Use this command to enable Open Shortest Path First (OSPF) routing for all IP interfaces on the router. Use the **no** form to disable it.

Syntax

router ospf
no router ospf

Command Mode

Global Configuration

Default Setting

Disabled

Command Usage

- OSPF is used to specify how routers exchange routing table information.
- This command is also used to enter router configuration mode.

Example

```
Console(config)#router ospf
Console(config-router)#
```

Related Commands

network area (4-255)

router-id

Use this command to assign a unique router ID for this device within the autonomous system. Use the **no** form to use the default router identification method (i.e., the lowest interface address).

Syntax

router-id *ip-address*

no router-id

ip-address - Router ID formatted as an IP address.

Command Mode

Router Configuration

Default Setting

Lowest interface address

Command Usage

- The router ID must be unique for every router in the autonomous system. Using the default setting based on the lowest interface address ensures that each router ID is unique. Also, note that you cannot set the router ID to 0.0.0.0 or 255.255.255.255.
- If this router already has registered neighbors, the new router ID will be used when the router is rebooted, or manually restarted by entering the **no router ospf** followed by the **router ospf** command.
- If the priority values of the routers bidding to be the designated router or backup designated router for an area are equal, the router with the highest ID is elected.

Example

```
Console(config-router)#router-id 10.1.1.1
Console(config-router)#
```

Related Commands

router ospf (4-246)

compatible rfc1583

Use this command to calculate summary route costs using RFC 1583 (OSPFv1). Use the **no** form to calculate costs using RFC 2328 (OSPFv2).

Syntax

compatible rfc1583
no compatible rfc1583

Command Mode

Router Configuration

Default Setting

RFC 1583 compatible

Command Usage

All routers in an OSPF routing domain should use the same RFC for calculating summary routes.

Example

```
Console(config-router)#compatible rfc1583
Console(config-router)#
```

default-information originate

Use this command to generate a default external route into an autonomous system. Use the **no** form to disable this feature.

Syntax

default-information originate [always] [metric *interface-metric*]
[metric-type *metric-type*]
no default-information originate

- **always** - Always advertise a default route to the local AS regardless of whether the router has a default route. (See “ip route” on page -227.)
- **interface-metric** - Metric assigned to the default route. (Range: 1-65535; Default: 10)
- **metric-type** - External link type used to advertise the default route. (Options: Type 1, Type 2; Default: Type 2)

Command Mode

Router Configuration

Default Setting

Disabled

Command Usage

- The metric for the default external route is used to calculate the path cost for traffic passed from other routers within the AS out through the ASBR.
- When you use this command to redistribute routes into a routing domain (i.e., an Autonomous System, this router automatically becomes an Autonomous System Boundary Router (ASBR). However, an ASBR does not, by default, generate a default route into the routing domain.
 - If you use the **always** keyword, the router will advertise itself as a default external route into the AS, even if a default external route does not actually exist. (To define a default route, use the **ip route** command.)
 - If you do *not* use the **always** keyword, the router can only advertise a default external route into the AS if the **redistribute** command is used to import external routes via RIP or static routing, and such a route is known.
- Type 1 route advertisements add the internal cost to the external route metric. Type 2 routes do not add the internal cost metric. When comparing Type 2 routes, the internal cost is only used as a tie-breaker if several Type 2 routes have the same cost.

Example

This example assigns a metric of 20 to the default external route advertised into an autonomous system, sending it as a Type 2 external metric.

```
Console(config-router)#default-information originate metric 20
metric-type 2
Console(config-router)#
```

Related Commands

ip route (4-227)
redistribute (4-254)

timers spf

Use this command to configure the hold time between making two consecutive shortest path first (SPF) calculations. Use the **no** form to restore the default value.

Syntax

timers spf *spf-holdtime*

no timers spf

spf-holdtime - Minimum time between two consecutive SPF calculations. (Range: 0-65535 seconds)

Command Mode

Router Configuration

Default Setting

10 seconds

Command Usage

- Setting the SPF holdtime to 0 means that there is no delay between consecutive calculations.
- Using a low value allows the router to switch to a new path faster, but uses more CPU processing time.

Example

```
Console(config-router)#timers spf 20
Console(config-router)#
```


area range

Use this command to summarize the routes advertised by an Area Border Router (ABR). Use the **no** form to disable this function.

Syntax

area *area-id* **range** *ip-address netmask* [**advertise** | **not-advertise**]
no area *area-id* **range** *ip-address netmask* [**advertise** | **not-advertise**]

- *area-id* - Identifies an area for which the routes are summarized. (The area ID must be in the form of an IP address.)
- *ip-address* - Base address for the routes to summarize.
- *netmask* - Network mask for the summary route.
- **advertise** - Advertises the specified address range.
- **not-advertise** - The summary is not sent, and the routes remain hidden from the rest of the network.

Command Mode

Router Configuration

Default Setting

Disabled

Command Usage

- This command can be used to advertise routes between areas.
- If routes are set to be advertised, the router will issue a Type 3 summary LSA for each address range specified with this command.
- This router supports up to 64 summary routes for area ranges.

Example

This example creates a summary address for all area routes in the range of 10.2.x.x.

```
Console(config-router)#area 10.2.0.0 range 10.2.0.0 255.255.0.0  
advertise  
Console(config-router)#
```

area default-cost

Use this command to specify a cost for the default summary route sent into a stub or not-so-stubby area (NSSA) from an Area Border Router (ABR). Use the **no** form to remove the assigned default cost.

Syntax

area *area-id* **default-cost** *cost*

no area *area-id* **default-cost**

- *area-id* - Identifier for a stub or NSSA, in the form of an IP address.
- *cost* - Cost for the default summary route sent to a stub or NSSA.
(Range: 0-65535)

Command Mode

Router Configuration

Default Setting

1

Command Usage

- If you enter this command for a normal area, it will changed to a stub.
- If the default cost is set to “0,” the router will not advertise a default route into the attached stub or NSSA.

Example

```
Console(config-router)#area 10.3.9.0 default-cost 10
Console(config-router)#
```

Related Commands

area stub (4-257)

summary-address

Use this command to aggregate routes learned from other protocols. Use the **no** form to remove a summary address.

Syntax

summary-address *summary-address netmask*

no summary-address *summary-address netmask*

- *summary-address* - Summary address covering a range of addresses.
- *netmask* - Network mask for the summary route.

Command Mode

Router Configuration

Default Setting

Disabled

Command Usage

- An Autonomous System Boundary Router (ASBR) can redistribute routes learned from other protocols by advertising an aggregate route into all attached autonomous systems.
- This router supports up to 16 Type-5 summary routes.

Example

This example creates a summary address for all routes contained in 192.168.x.x.

```
Console(config-router)#summary-address 192.168.0.0 255.255.0.0
Console(config-router)#
```

Related Commands

area range (4-251)

redistribute

Use this command to import external routing information from other routing domains (i.e., protocols) into the autonomous system. Use the **no** form to disable this feature.

Syntax

redistribute [**rip** | **static**] [**metric** *metric-value*] [**metric-type** *type-value*]
no redistribute [**rip** | **static**] [**metric** *metric-value*] [**metric-type** *type-value*]

- **rip** - External routes will be imported from the Routing Information Protocol into this Autonomous System.
- **static** - Static routes will be imported into this Autonomous System.
- *metric-value* - Metric assigned to all external routes for the specified protocol. (Range: 1-65535; Default: 10)
- *type-value*
 - **1** - Type 1 external route
 - **2** - Type 2 external route (default) - Routers do not add internal route metric to external route metric.

Command Mode

Router Configuration

Default Setting

redistribution - none
protocol - RIP and static
metric-value - 0
type-metric - 2

Command Usage

- This router supports redistribution for both RIP and static routes.
- When you redistribute external routes into an OSPF autonomous system (AS), the router automatically becomes an autonomous system boundary router (ASBR). If the **redistribute** command is used in conjunction with the **default-information originate** command to generate a “default” external route into the AS, the metric value specified in this command supersedes the metric specified in the **default-information originate** command.

- Metric type specifies the way to advertise routes to destinations outside the AS via External LSAs. Specify Type 1 to add the internal cost metric to the external route metric. In other words, the cost of the route from any router within the AS is equal to the cost associated with reaching the advertising ASBR, plus the cost of the external route. Specify Type 2 to only advertise the external route metric.

Example

This example redistributes routes learned from RIP as Type 1 external routes.

```
Console(config-router)#redistribute rip metric-type 1
Console(config-router)#
```

Related Commands

default-information originate (4-248)

network area

Use this command to define an OSPF area and the interfaces that operate within this area. Use the **no** form to disable OSPF for a specified interface.

Syntax

network *ip-address netmask area area-id*

no network *ip-address netmask area area-id*

- *ip-address* - Address of the interfaces to add to the area.
- *netmask* - Network mask of the address range to add to the area.
- *area-id* - Area to which the specified address or range is assigned. An OSPF area identifies a group of routers that share common routing information. (The area ID must be in the form of an IP address.)

Command Mode

Router Configuration

Default Setting

Disabled

Command Usage

- An area ID uniquely defines an OSPF broadcast area. The area ID 0.0.0.0 indicates the OSPF backbone for an autonomous system. Each router must be connected to the backbone via a direct connection or a virtual link.
- Set the area ID to the same value for all routers on a network segment using the network mask to add one or more interfaces to an area.
- Be sure to include the primary address for an interface in the network area, otherwise, OSPF will not operate for any secondary addresses covered by the command.
- An interface can only be assigned to a single area. If an address range is overlapped in subsequent network area commands, the router will implement the address range for the area specified in first command, and ignore the overlapping ranges in subsequent commands. However, note that if a more specific address range is removed from an area, the interface belonging to that range may still remain active if a less specific address range covering that area has been specified.
- This router supports up to 64 OSPF router interfaces, and up to 16 total areas (either normal transit areas, stubs, or NSSAs).

Example

This example creates the backbone 0.0.0.0 covering class B addresses 10.1.x.x, and a normal transit area 10.2.9.0 covering the class C addresses 10.2.9.x.

```
Console(config-router)#network 10.1.0.0 255.255.0.0 area 0.0.0.0
Console(config-router)#network 10.2.9.0 255.255.255.0 area 10.1.0.0
Console(config-router)#
```

area stub

Use this command to define a stub area. To remove a stub, use the **no** form without the optional keyword. To remove the summary attribute, use the **no** form with the summary keyword.

Syntax

area *area-id* **stub** [**summary**]

no area *area-id* **stub** [**summary**]

- *area-id* - Identifies the stub area.
(The area ID must be in the form of an IP address.)
- **summary** - Makes an Area Border Router (ABR) send a summary link advertisement into the stub area. (Default: no summary)

Command Mode

Router Configuration

Default Setting

No stub is configured.

Command Usage

- All routers in a stub must be configured with the same area ID.
- Routing table space is saved in a stub by blocking Type-4 AS summary LSAs and Type 5 external LSAs. The default setting for this command completely isolates the stub by blocking Type-3 summary LSAs that advertise the default route for destinations external to the local area or the autonomous system.
- Use the **area default-cost** command to specify the cost of a default summary route sent into a stub by an ABR.
- This router supports up to 16 total areas (either normal transit areas, stubs, or NSSAs).

Example

This example creates a stub area 10.2.0.0, and assigns all interfaces with class B addresses 10.2.x.x to the stub.

```
Console(config-router)#area 10.2.0.0 stub
Console(config-router)#network 10.2.0.0 0.255.255.255 area 10.2.0.0
Console(config-router)#
```

Related Commands

area default-cost (4-252)

area nssa

Use this command to define a not-so-stubby area (NSSA). To remove an NSSA, use the **no** form without any optional keywords. To remove an optional attribute, use the **no** form without the relevant keyword.

Syntax

area *area-id* **nssa** [**no-redistribution**] [**default-information-originate**]
no area *area-id* **nssa** [**no-redistribution**]
[**default-information-originate**]

- *area-id* - Identifies the NSSA.
(The area ID must be in the form of an IP address.)
- **no-redistribution** - Use this keyword when the router is an NSSA Area Border Router (ABR) and you want the **redistribute** command to import routes only into normal areas, and not into the NSSA. In other words, this keyword prevents the NSSA ABR from advertising external routing information (learned via routers in other areas) into the NSSA.
- **default-information-originate** - When the router is an NSSA Area Border Router (ABR) or an NSSA Autonomous System Boundary Router (ASBR), this parameter causes it to generate Type-7 default LSA into the NSSA. This default provides a route to other areas within the AS for an NSSA ABR, or to areas outside the AS for an NSSA ASBR.

Command Mode

Router Configuration

Default Setting

No NSSA is configured.

Command Usage

- All routers in a NSSA must be configured with the same area ID.
- An NSSA is similar to a stub, because when the router is an ABR, it can send a default route for other areas in the AS into the NSSA using the **default-information-originate** keyword. However, an NSSA is different from a stub, because when the router is an ASBR, it can import a default external AS route (for routing protocol domains adjacent to the NSSA but not within the OSPF AS) into the NSSA using the **default-information-originate** keyword.
- External routes advertised into an NSSA can include network destinations outside the AS learned via OSPF, the default route, static routes, routes imported from other routing protocols such as RIP, and networks directly connected to the router that are not running OSPF.
- NSSA external LSAs (Type 7) are converted by any ABR adjacent to the NSSA into external LSAs (Type-5), and propagated into other areas within the AS.
- Also, note that unlike stub areas, all Type-3 summary LSAs are always imported into NSSAs to ensure that internal routes are always chosen over Type-7 NSSA external routes.
- This router supports up to 16 total areas (either normal transit areas, stubs, or NSSAs).

Example

This example creates a stub area 10.3.0.0, and assigns all interfaces with class B addresses 10.3.x.x to the NSSA. It also instructs the router to generate external LSAs into the NSSA when it is an NSSA ABR or NSSA ASBR.

```
Console(config-router)#area 10.3.0.0 nssa
  default-information-originate
Console(config-router)#network 10.3.0.0 255.255.0.0 area 10.2.0.0
Console(config-router)#
```

area virtual-link

Use this command to define a virtual link. To remove a virtual link, use the **no** form with no optional keywords. To restore the default value for an attribute, use the **no** form with the required keyword.

Syntax

```
area area-id virtual-link router-id
    [authentication [message-digest | null ]] [hello-interval seconds]
    [retransmit-interval seconds] [transmit-delay seconds] [dead-interval
seconds] [[authentication-key key] | [message-digest-key key-id
md5 key]]
```

```
no area area-id virtual-link router-id
    [authentication [message-digest | null ]] [hello-interval seconds]
    [retransmit-interval seconds] [transmit-delay seconds] [dead-interval
seconds] [[authentication-key key] | [message-digest-key key-id
md5 key]]
```

no area *area-id*

- *area-id* - Identifies the transit area for the virtual link. (The area ID must be in the form of an IP address.)
- *router-id* - Router ID of the virtual link neighbor. This must be an Area Border Router (ABR) that is adjacent to both the backbone and the transit area at the other end of the virtual link.
- **authentication** - Specifies the authentication mode. If no optional parameters follow this keyword, then plain text authentication is used along with the password specified by the **authentication-key**. If **message-digest** authentication is specified, then the **message-digest-key** and **md5** parameters must also be specified. If the **null** option is specified, then no authentication is performed on any OSPF routing protocol messages.
- **message-digest** - Specifies message-digest (MD5) authentication.
- **null** - Indicates that no authentication is used.
- **hello-interval** *seconds* - Specifies the transmit delay between sending hello packets. Setting the hello interval to a smaller value can reduce the delay in detecting topological changes, but will increase the routing traffic. This value must be the same for all routers attached

to an autonomous system. (Range: 1-65535 seconds; Default: 10 seconds)

- **retransmit-interval** *seconds* - Specifies the interval at which the ABR retransmits link-state advertisements (LSA) over the virtual link. The retransmit interval should be set to a conservative value that provides an adequate flow of routing information, but does not produce unnecessary protocol traffic. However, note that this value should be larger for virtual links. (Range: 1-3600 seconds; Default: 5 seconds)
- **transmit-delay** *seconds* - Estimates the time required to send a link-state update packet over the virtual link, considering the transmission and propagation delays. LSAs have their age incremented by this amount before transmission. This value must be the same for all routers attached to an autonomous system. (Range: 1-3600 seconds; Default: 1 seconds)
- **dead-interval** *seconds* - Specifies the time that neighbor routers will wait for a hello packet before they declare the router down. This value must be the same for all routers attached to an autonomous system. (Range: 1-65535 seconds; Default: 4 x hello interval, or 40 seconds)
- **authentication-key** *key* - Sets a plain text password (up to 8 characters) that is used by neighboring routers on a virtual link to generate or verify the authentication field in protocol message headers. A separate password can be assigned to each network interface. However, this key must be the same for all neighboring routers on the same network (i.e., autonomous system). This key is only used when authentication is enabled for the backbone.
- **message-digest-key** *key-id md5 key* - Sets the key identifier and password to be used to authenticate protocol messages passed between neighboring routers and this router when using message digest (MD5) authentication. The *key-id* is an integer from 1-255, and the *key* is an alphanumeric string up to 16 characters long. If MD5 authentication is used on a virtual link, then it must be enabled on all routers within an autonomous system; and the key identifier and key must also be the same for all routers.

Command Mode

Router Configuration

Default Setting

area-id: None

router-id: None

hello-interval: 10 seconds

retransmit-interval: 5 seconds

transmit-delay: 1 second

dead-interval: 40 seconds

authentication-key: None

message-digest-key: None

Command Usage

- All areas must be connected to a backbone area (0.0.0.0) to maintain routing connectivity throughout the autonomous system. If it not possible to physically connect an area to the backbone, you can use a virtual link. A virtual link can provide a logical path to the backbone for an isolated area. You can specify up to 32 virtual links on this router.
- Any area disconnected from the backbone must include the transit area ID and the router ID for a virtual link neighbor that is adjacent to the backbone.
- This router supports up to 64 virtual links.

Example

This example creates a virtual link using the defaults for all optional parameters.

```
Console(config-router)#network 10.4.0.0 0.255.255.0.0 area 10.4.0.0
Console(config-router)#area 10.4.0.0 virtual-link 10.4.3.254
Console(config-router)#
```

This example creates a virtual link using MD5 authentication.

```
Console(config-router)#network 10.4.0.0 0.255.255.0.0 area 10.4.0.0
Console(config-router)#area 10.4.0.0 virtual-link 10.4.3.254
message-digest-key 5 md5 ld83jdpq
Console(config-router)#
```

Related Commands

show ip ospf virtual-links (4-284)

ip ospf authentication

Use this command to specify the authentication type used for an interface. Enter this command without any optional parameters to specify plain text (or simple password) authentication. Use the **no** form to restore the default of no authentication.

Syntax

ip ospf authentication [message-digest | null]
no ip ospf authentication

- **message-digest** - Specifies message-digest (MD5) authentication.
- **null** - Indicates that no authentication is used.

Command Mode

Interface Configuration (VLAN)

Default Setting

No authentication

Command Usage

- Before specifying plain-text password authentication for an interface, configure a password with the **ip ospf authentication-key** command. Before specifying MD5 authentication for an interface, configure the message-digest key-id and key with the **ip ospf message-digest-key** command.
- The plain-text authentication-key, or the MD5 key-id and key, must be used consistently throughout the autonomous system.

Example

This example enables message-digest authentication for the specified interface.

```
Console(config)#interface vlan 1
Console(config-if)#ip ospf authentication message-digest
Console(config-if)#
```

Related Commands

ip ospf authentication-key (4-264)
ip ospf message-digest-key (4-265)

ip ospf authentication-key

Use this command to assign a simple password to be used by neighboring routers. Use the **no** form to remove the password.

Syntax

ip ospf authentication-key *key*

no ip ospf authentication-key

key - Sets a plain text password. (Range: 1-8 characters)

Command Mode

Interface Configuration (VLAN)

Default Setting

No password

Command Usage

- Before specifying plain-text password authentication for an interface, configure a password with the **ip ospf authentication-key** command. Before specifying MD5 authentication for an interface, configure the message-digest key-id and key with the **ip ospf message-digest-key** command.
- A different password can be assigned to each network interface basis, but the password must be used consistently on all neighboring routers throughout a network (i.e., autonomous system).

Example

This example sets a password for the specified interface.

```
Console(config)#interface vlan 1
Console(config-if)#ip ospf authentication-key badboy
Console(config-if)#
```

Related Commands

ip ospf authentication (4-263)

ip ospf message-digest-key

Use this command to enable message-digest (MD5) authentication on the specified interface and to assign a key-id and key to be used by neighboring routers. Use the **no** form to remove an existing key.

Syntax

ip ospf message-digest-key *key-id* **md5** *key*

no ip ospf message-digest-key *key-id*

- *key-id* - Index number of an MD5 key. (Range: 1-255)
- *key* - Alphanumeric password used to generate a 128 bit message digest or “fingerprint.” (Range: 1-16 characters)

Command Mode

Interface Configuration (VLAN)

Default Setting

MD5 authentication is disabled.

Command Usage

- Normally, only one key is used per interface to generate authentication information for outbound packets and to authenticate incoming packets. Neighbor routers must use the same key identifier and key value.
- When changing to a new key, the router will send multiple copies of all protocol messages, one with the old key and another with the new key. Once all the neighboring routers start sending protocol messages back to this router with the new key, the router will stop using the old key. This rollover process gives the network administrator time to update all the routers on the network without affecting the network connectivity. Once all the network routers have been updated with the new key, the old key should be removed for security reasons.

Example

This example sets a message-digest key identifier and password.

```
Console(config)#interface vlan 1
Console(config-if)#ip ospf message-digest-key 1 md5 aiebel
Console(config-if)#
```

Related Commands

ip ospf authentication (4-263)

ip ospf cost

Use this command to explicitly set the cost of sending a packet on an interface. Use the **no** form to restore the default value.

Syntax

ip ospf cost *cost*

no ip ospf cost

cost - Link metric for this interface. Use higher values to indicate slower ports. (Range: 1-65535)

Command Mode

Interface Configuration (VLAN)

Default Setting

1

Command Usage

Interface cost reflects the port speed. This router uses a default cost of 1 for all ports. Therefore, if you install a Gigabit module, you may have to reset the cost for all of the 100 Mbps ports to a value greater than 1.

Example

```
Console(config)#interface vlan 1
Console(config-if)#ip ospf cost 10
Console(config-if)#
```


ip ospf dead-interval

Use this command to set the interval at which hello packets are not seen before neighbors declare the router down. Use the **no** form to restore the default value.

Syntax

ip ospf dead-interval *seconds*

no ip ospf dead-interval

seconds - The maximum time that neighbor routers can wait for a hello packet before declaring the transmitting router down. This interval must be set to the same value for all routers on the network. (Range: 1-65535)

Command Mode

Interface Configuration (VLAN)

Default Setting

40, or four times the interval specified by the **ip ospf hello-interval** command.

Example

```
Console(config)#interface vlan 1
Console(config-if)#ip ospf dead-interval 50
Console(config-if)#
```

Related Commands

ip ospf hello-interval (4-268)

ip ospf hello-interval

Use this command to specify the interval between sending hello packets on an interface. Use the **no** form to restore the default value.

Syntax

ip ospf hello-interval *seconds*

no ip ospf hello-interval

seconds - Interval at which hello packets are sent from an interface. This interval must be set to the same value for all routers on the network. (Range: 1-65535)

Command Mode

Interface Configuration (VLAN)

Default Setting

10 seconds

Command Usage

Hello packets are used to inform other routers that the sending router is still active. Setting the hello interval to a smaller value can reduce the delay in detecting topological changes, but will increase routing traffic.

Example

```
Console(config)#interface vlan 1
Console(config-if)#ip ospf hello-interval 5
Console(config-if)#
```

ip ospf priority

Use this command to set the router priority used when determining the designated router (DR) and backup designated router (BDR) for an area. Use the **no** form to restore the default value.

Syntax

ip ospf priority *priority*

no ip ospf priority

priority - Sets the interface priority for this router. (Range: 0-255)

Command Mode

Interface Configuration (VLAN)

Default Setting

1

Command Usage

- Set the priority to zero to prevent a router from being elected as a DR or BDR. If set to any value other than zero, the router with the highest priority will become the DR and the router with the next highest priority becomes the BDR. If two or more routers are tied with the same highest priority, the router with the higher ID will be elected.
- If a DR already exists for an area when this interface comes up, the new router will accept the current DR regardless of its own priority. The DR will not change until the next time the election process is initiated.

Example

```
Console(config)#interface vlan 1
Console(config-if)#ip ospf priority 5
Console(config-if)#
```

ip ospf retransmit-interval

Use this command to specify the time between resending link-state advertisements (LSAs). Use the **no** form to restore the default value.

Syntax**ip ospf retransmit-interval** *seconds***no ip ospf retransmit-interval**

seconds - Sets the interval at which LSAs are retransmitted from this interface. (Range: 1-65535)

Command Mode

Interface Configuration (VLAN)

Default Setting

5 seconds

Command Usage

A router will resend an LSA to a neighbor if it receives no acknowledgment. The retransmit interval should be set to a conservative value that provides an adequate flow of routing information, but does not produce unnecessary protocol traffic. Note that this value should be larger for virtual links.

Example

```
Console(config)#interface vlan 1
Console(config-if)#ip ospf retransmit-interval 7
Console(config-if)#
```

ip ospf transmit-delay

Use this command to set the estimated time to send a link-state update packet over an interface. Use the **no** form to restore the default value.

Syntax

ip ospf transmit-delay *seconds*

no ip ospf transmit-delay

seconds - Sets the estimated time required to send a link-state update.
(Range: 1-65535)

Command Mode

Interface Configuration (VLAN)

Default Setting

1 second

Command Usage

LSAs have their age incremented by this delay before transmission. When estimating the transmit delay, consider both the transmission and propagation delays for an interface. Set the transmit delay according to link speed, using larger values for lower-speed links. The transmit delay must be the same for all routers attached to an autonomous system.

Example

```
Console(config)#interface vlan 1
Console(config-if)#ip ospf transmit-delay 6
Console(config-if)#
```

show ip ospf

Use this command to show basic information about the routing configuration.

Command Mode

Privileged Exec

Example

```
Console#show ip ospf
Routing Process with ID 10.1.1.253
Supports only single TOS(TOS0) route
It is an area border and autonomous system boundary router
Redistributing External Routes from,
    rip with metric mapped to 10
Number of area in this router is 2
Area 0.0.0.0 (BACKBONE)
    Number of interfaces in this area is 1
    SPF algorithm executed 19 times
Area 10.1.0.0
    Number of interfaces in this area is 4
    SPF algorithm executed 19 times
Console#
```

Field	Description
Routing Process with ID	Router ID
Supports only single TOS (TOS0) route	Type of service is not supported, so you can only assign one cost per interface
It is an <i>router type</i>	The types displayed include internal, area border, or autonomous system boundary routers
Number of areas in this router	The number of configured areas
<i>Area identifier</i>	The area address, and area type if backbone, NSSA or stub
Number of interfaces	The number of interfaces attached to this area
SPF algorithm executed	The number of times the shortest path first algorithm has been executed for this area

show ip ospf border-routers

Use this command to show entries in the routing table that lead to an Area Border Router (ABR) or Autonomous System Boundary Router (ASBR).

Command Mode

Privileged Exec

Example

Console#show ip ospf border-routers						
Destination	Next Hop	Cost	Type	RteType	Area	SPF No
10.1.1.252	10.1.1.253	0	ABR	INTRA	10.1.0.0	3
10.2.6.252	10.2.9.253	0	ASBR	INTER	10.2.0.0	7
Console#						

Field	Description
Destination	Identifier for the destination router
Next Hop	IP address of the next hop toward the destination
Cost	Link metric for this route
Type	Router type of the destination; either ABR, ASBR or both
RteType	Route type; either intra-area or inter-area route (INTRA or INTER)
Area	The area from which this route was learned
SPF No	The number of times the shortest path first algorithm has been executed for this route

show ip ospf database

Use this command to show information about different OSPF Link State Advertisements (LSAs) stored in this router's database.

Syntax

```
show ip ospf [area-id] database [adv-router [ip-address]]
show ip ospf [area-id] database [asbr-summary] [link-state-id]
show ip ospf [area-id] database [asbr-summary] [link-state-id] [adv-router [ip-address]]
show ip ospf [area-id] database [asbr-summary] [link-state-id] [self-originate] [link-state-id]
show ip ospf [area-id] database [database-summary]
show ip ospf [area-id] database [external] [link-state-id]
show ip ospf [area-id] database [external] [link-state-id] [adv-router [ip-address]]
show ip ospf [area-id] database [external] [link-state-id] [self-originate] [ip-address]
show ip ospf [area-id] database [network] [link-state-id]
show ip ospf [area-id] database [network] [link-state-id] [adv-router [ip-address]]
show ip ospf [area-id] database [network] [link-state-id] [self-originate] [link-state-id]
show ip ospf [area-id] database [nssa-external] [link-state-id]
show ip ospf [area-id] database [nssa-external] [link-state-id] [adv-router [ip-address]]
show ip ospf [area-id] database [nssa-external] [link-state-id] [self-originate] [link-state-id]
show ip ospf [area-id] database [router] [link-state-id]
show ip ospf [area-id] database [router] [adv-router [ip-address]]
show ip ospf [area-id] database [router] [self-originate] [link-state-id]
show ip ospf [area-id] database [self-originate] [link-state-id]
show ip ospf [area-id] database [summary] [link-state-id]
show ip ospf [area-id] database [summary] [link-state-id] [adv-router [ip-address]]
show ip ospf [area-id] database [summary] [link-state-id] [self-originate] [link-state-id]
```

- *area-id* - Area defined for which you want to view LSA information. (This item must be entered in the form of an IP address.)
- **adv-router** - IP address of the advertising router. If not entered, information about all advertising routers is displayed.
- *ip-address* - IP address of the specified router. If no address is entered, information about the local router is displayed.
- **asbr-summary** - Shows information about Autonomous System Boundary Router summary LSAs.
- *link-state-id* - The network portion described by an LSA. The *link-state-id* entered should be:
 - An IP network number for Type 3 Summary and External LSAs
 - A Router ID for Router, Network, and Type 4 AS Summary LSAs

Also, note that when an Type 5 ASBR External LSA is describing a default route, its *link-state-id* is set to the default destination (0.0.0.0).

- **self-originate** - Shows LSAs originated by this router.
- **database-summary** - Shows a count for each LSA type for each area stored in the database, and the total number of LSAs in the database.
- **external** - Shows information about external LSAs.
- **network** - Shows information about network LSAs.
- **nssa-external** - Shows information about NSSA external LSAs.
- **router** - Shows information about router LSAs.
- **summary** - Shows information about summary LSAs.

Command Mode

Privileged Exec

Examples

The following shows output for the **show ip ospf database** command.

```
Console#show ip ospf database

      Displaying Router Link States(Area 10.1.0.0)
      Link ID      ADV Router    Age      Seq#      Checksum
      -----
      10.1.1.252    10.1.1.252    26      0X80000005    0X89A1
      10.1.1.253    10.1.1.253    23      0X80000002    0X8D9D

      Displaying Net Link States(Area 10.1.0.0)
      Link ID      ADV Router    Age      Seq#      Checksum
      -----
      10.1.1.252    10.1.1.252    28      0X80000001    0X53E1
Console#
```

Field	Description
Link ID	Router ID
ADV Router	Advertising router ID
Age	Age of LSA (in seconds)
Seq#	Sequence number of LSA (used to detect older duplicate LSAs)
Checksum	Checksum of the complete contents of the LSA

The following shows output when using the **asbr-summary** keyword.

```

Console#show ip ospf database asbr-summary

OSPF Router with id(10.1.1.253)

    Displaying Summary ASB Link States(Area 0.0.0.0)

LS age: 433
Options: (No TOS-capability)
LS Type: Summary Links (AS Boundary Router)
Link State ID: 192.168.5.1 (AS Boundary Router's Router ID)
Advertising Router: 192.168.1.5
LS Sequence Number: 80000002
LS Checksum: 0x51E2
Length: 32
Network Mask: 255.255.255.0
Metric: 1

Console#

```

Field	Description
OSPF Router id	Router ID
LS age	Age of LSA (in seconds)
Options	Optional capabilities associated with the LSA
LS Type	Summary Links - LSA describes routes to AS boundary routers
Link State ID	Interface address of the autonomous system boundary router
Advertising Router	Advertising router ID
LS Sequence Number	Sequence number of LSA (used to detect older duplicate LSAs)
LS Checksum	Checksum of the complete contents of the LSA
Length	The length of the LSA in bytes
Network Mask	Address mask for the network
Metrics	Cost of the link

The following shows output when using the **database-summary** keyword.

```
Console#show ip ospf database database-summary

Area ID (10.1.0.0)
  Router      Network      Sum-Net      Sum-ASBR      External-AS      External-Nssa
    2          1          1          0          0          0
Total LSA Counts : 4
Console#
```

Field	Description
Area ID	Area identifier
Router	Number of router LSAs
Network	Number of network LSAs
Sum-Net	Number of summary LSAs
Sum-ASBR	Number of summary ASBR LSAs
External-AS	Number of autonomous system external LSAs
External-Nssa	Number of NSSA external network LSAs
Total LSA Counts	Total number of LSAs

The following shows output when using the **external** keyword.

```
Console#show ip ospf database external

OSPF Router with id(192.168.5.1) (Autonomous system 5)

      Displaying AS External Link States

LS age: 433
Options: (No TOS-capability)
LS Type: AS External Link
Link State ID: 10.1.1.253 (External Network Number)
Advertising Router: 10.1.2.254
LS Sequence Number: 80000002
LS Checksum: 0x51E2
Length: 32
Network Mask: 255.255.0.0
Metric Type: 2 (Larger than any link state path)
Metric: 1
Forward Address: 0.0.0.0
External Route Tag: 0

Console#
```

Field	Description
OSPF Router id	Router ID
LS age	Age of LSA (in seconds)
Options	Optional capabilities associated with the LSA
LS Type	AS External Links - LSA describes routes to destinations outside the AS (including default external routes for the AS)
Link State ID	IP network number (External Network Number)
Advertising Router	Advertising router ID
LS Sequence Number	Sequence number of LSA (used to detect older duplicate LSAs)
LS Checksum	Checksum of the complete contents of the LSA
Length	The length of the LSA in bytes
Network Mask	Address mask for the network
Metric Type	Type 1 or Type 2 external metric (see “redistribute” on page -254)
Metrics	Cost of the link
Forward Address	Forwarding address for data to be passed to the advertised destination (If set to 0.0.0.0, data is forwarded to the originator of the advertisement)
External Route Tag	32-bit field attached to each external route (Not used by OSPF; may be used to communicate other information between boundary routers as defined by specific applications)

The following shows output when using the **network** keyword.

```
Console#show ip ospf database network

OSPF Router with id(10.1.1.253)

    Displaying Net Link States(Area 10.1.0.0)

Link State Data Network (Type 2)
-----

LS age: 433
Options: Support External routing capability
LS Type: Network Links
Link State ID: 10.1.1.252
(IP interface address of the Designated Router)
Advertising Router: 10.1.1.252
LS Sequence Number: 80000002
LS Checksum: 0x51E2
Length: 32
Network Mask: 255.255.255.0

    Attached Router: 10.1.1.252
    Attached Router: 10.1.1.253
Console#
```

Field	Description
OSPF Router id	Router ID
LS age	Age of LSA (in seconds)
Options	Optional capabilities associated with the LSA
LS Type	Network Link - LSA describes the routers attached to the network
Link State ID	Interface address of the designated router
Advertising Router	Advertising router ID
LS Sequence Number	Sequence number of LSA (used to detect older duplicate LSAs)
LS Checksum	Checksum of the complete contents of the LSA
Length	The length of the LSA in bytes
Network Mask	Address mask for the network
Attached Router	List of routers attached to the network; i.e., fully adjacent to the designated router, including the designated router itself

The following shows output when using the **router** keyword.

```

Console#show ip ospf database router

OSPF Router with id(10.1.1.253)

    Displaying Router Link States(Area 10.1.0.0)

Link State Data Router (Type 1)
-----

LS age: 233
Options: Support External routing capability
LS Type: Router Links
Link State ID: 10.1.1.252 (Originating Router's Router ID)
Advertising Router: 10.1.1.252
LS Sequence Number: 80000011
LS Checksum: 0x7287
Length: 48
Router Role: Area Border Router
Number of Links: 1
-----
Link ID: 10.1.7.0 (IP Network/Subnet Number)
  Link Data: 255.255.255.0 (Network's IP address mask)
  Link Type: Connection to a stub network
  Number of TOS metrics: 0
  Metrics: 1

Console#

```

Field	Description
OSPF Router id	Router ID
LS age	Age of LSA (in seconds)
Options	Optional capabilities associated with the LSA
LS Type	Router Link - LSA describes the router's interfaces.
Link State ID	Router ID of the router that originated the LSA
Advertising Router	Advertising router ID
LS Sequence Number	Sequence number of LSA (used to detect older duplicate LSAs)
LS Checksum	Checksum of the complete contents of the LSA
Length	The length of the LSA in bytes
Router Role	Description of router type, including: None, AS Boundary Router, Area Border Router, or Virtual Link
Number of Links	Number of links described by the LSA

Field	Description
Link ID	Link type and corresponding Router ID or network address
Link Data	<ul style="list-style-type: none"> • Router ID for transit network • Network's IP address mask for stub network • Neighbor Router ID for virtual link
Link Type	Link-state type, including transit network, stub network, or virtual link
Number of TOS metrics	Type of Service metric – This router only supports TOS 0 (or normal service)
Metrics	Cost of the link

The following shows output when using the **summary** keyword.

```

Console#show ip ospf database summary

OSPF Router with id(10.1.1.253)

    Displaying Summary Net Link States(Area 10.1.0.0)

Link State Data Summary (Type 3)
-----

LS age: 686
Options: Support External routing capability
LS Type: Summary Links(Network)
Link State ID: 10.2.6.0 (The destination Summary Network Number)
Advertising Router: 10.1.1.252
LS Sequence Number: 80000003
LS Checksum: 0x3D02
Length: 28
Network Mask: 255.255.255.0
Metric: 1

Console#

```

Field	Description
OSPF Router id	Router ID
LS age	Age of LSA (in seconds)
Options	Optional capabilities associated with the LSA
LS Type	Summary Links - LSA describes routes to networks
Link State ID	Router ID of the router that originated the LSA
Advertising Router	Advertising router ID

Field	Description
LS Sequence Number	Sequence number of LSA (used to detect older duplicate LSAs)
LS Checksum	Checksum of the complete contents of the LSA
Length	The length of the LSA in bytes
Network Mask	Destination network's IP address mask
Metrics	Cost of the link

show ip ospf interface

Use this command to display summary information for OSPF interfaces.

Syntax

show ip ospf interface [**vlan** *vlan-id*]
vlan-id - VLAN ID (Range: 1-4094)

Command Mode

Privileged Exec

Example

```

Console#show ip ospf interface vlan 1

Vlan 1 is up
  Interface Address 10.1.1.253, Mask 255.255.255.0, Area 10.1.0.0
  Router ID 10.1.1.253, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State BDR, Priority 1
  Designated Router id 10.1.1.252, Interface address 10.1.1.252
  Backup Designated router id 10.1.1.253, Interface addr 10.1.1.253
  Timer intervals configured, Hello 10, Dead 40, Retransmit 5

Console#

```

Field	Description
Vlan	VLAN ID and Status of physical link
Interface Address	IP address of OSPF interface
Mask	Network mask for interface address
Area	OSPF area to which this interface belongs
Router ID	Router ID
Network Type	Includes broadcast, non-broadcast, or point-to-point networks

Field	Description
Cost	Interface transmit cost
Transmit Delay	Interface transmit delay (in seconds)
State	<ul style="list-style-type: none">• Disabled – OSPF not enabled on this interface• Down – OSPF is enabled on this interface, but interface is down• Loopback – This is a loopback interface• Waiting – Router is trying to find the DR and BDR• DR – Designated Router
State (continued)	<ul style="list-style-type: none">• BDR – Backup Designated Router• DRother – Interface is on a multiaccess network, but is not the DR or BDR
Priority	Router priority
Designated Router	Designated router ID and respective interface address
Backup Designated Router	Backup designated router ID and respective interface address
Timer intervals	Configuration settings for timer intervals, including Hello, Dead and Retransmit

show ip ospf neighbor

Use this command to display information about neighboring routers on each interface within an OSPF area.

Syntax

show ip ospf neighbor

Command Mode

Privileged Exec

Example

```
Console#show ip ospf neighbor

      ID                Pri          State          Address
-----
  10.1.1.252           1          FULL/DR       10.1.1.252

Console#
```


Field	Description
ID	Neighbor's router ID
Pri	Neighbor's router priority
State	<p>OSPF state and identification flag</p> <p>States include:</p> <p>Down – Connection down</p> <p>Attempt – Connection down, but attempting contact (for non-broadcast networks)</p> <p>Init – Have received Hello packet, but communications not yet established</p> <p>Two-way – Bidirectional communications established</p> <p>ExStart – Initializing adjacency between neighbors</p> <p>Exchange – Database descriptions being exchanged</p> <p>Loading – LSA databases being exchanged</p> <p>Full – Neighboring routers now fully adjacent</p> <p>Identification flags include:</p> <p>D – Dynamic neighbor</p> <p>S – Static neighbor</p> <p>DR – Designated router</p> <p>BDR – Backup designated router</p>
Address	IP address of this interface

show ip ospf summary-address

Use this command to display all summary address information.

Syntax

show ip ospf summary-address

Command Mode

Privileged Exec

Example

This example shows a summary address and associated network mask.

```

Console#show ip ospf summary-address
10.1.0.0/255.255.0.0
Console#

```

Related Commands

summary-address (4-253)

show ip ospf virtual-links

Use this command to display detailed information about virtual links.

Syntax

show ip ospf virtual-links

Command Mode

Privileged Exec

Example

```
Console#show ip ospf virtual-links
Virtual Link to router 10.1.1.253 is up
Transit area 10.1.1.0
Transmit Delay is 1 sec
Timer intervals configured, Hello 10, Dead 40, Retransmit 5
Console#
```

Field	Description
Virtual Link to router	OSPF neighbor and link state (up or down)
Transit area	Common area the virtual link crosses to reach the target router
Transmit Delay	Estimated transmit delay (in seconds) on the virtual link
Timer intervals	Configuration settings for timer intervals, including Hello, Dead and Retransmit

Related Commands

area virtual-link (4-260)

Multicast Routing Commands

This router uses IGMP snooping and query to determine the ports connected to downstream multicast hosts, and to propagate this information back up through the multicast tree to ensure that requested services are forwarded through each intermediate node between the multicast server and its hosts, and also to filter traffic from all of the other interfaces that do not require these services.

Multicast routers use snooping and query messages, along with a multicast routing protocol to deliver IP multicast packets across different subnetworks. This router supports both the Distance-Vector Multicast Routing Protocol (DVMRP) and Protocol Independent Multicasting (PIM). (Note that you should enable IGMP for any interface that is using multicast routing.)

Command Groups	Function	Page
Static Multicast Routing	Configures static multicast router ports	4-285
General Multicast Routing	Enables IP multicast routing globally; also displays the IP multicast routing table created from static and dynamic routing information	4-287
DVMRP Multicast Routing	Configures global and interface settings for DVMRP	4-290
PIM-DM Multicast Routing	Configures global and interface settings for PIM-DM	4-301

Static Multicast Routing Commands

Command	Function	Mode	Page
ip igmp snooping vlan mrouter	Adds a multicast router port	GC	4-286
show ip igmp snooping mrouter	Shows multicast router ports	PE	4-287

ip igmp snooping vlan mrouter

Use this command to statically configure a multicast router port. Use the **no** form to remove the configuration.

Syntax

ip igmp snooping vlan *vlan-id* mrouter *interface*
no ip igmp snooping vlan *vlan-id* mrouter *interface*

- *vlan-id* - VLAN ID (Range: 1-4094)
- *interface*
 - **ethernet** *unit/port*
 - *unit* - This is device 1.
 - *port* - Port number.
 - **port-channel** *channel-id* (Range: 1-6)

Default Setting

No static multicast router ports are configured.

Command Mode

Global Configuration

Command Usage

Depending on your network connections, IGMP snooping may not always be able to locate the IGMP querier. Therefore, if the IGMP querier is a known multicast router/switch connected over the network to an interface (port or trunk) on your router, you can manually configure that interface to join all the current multicast groups.

Example

The following shows how to configure port 11 as a multicast router port within VLAN 1:

```
Console(config)#ip igmp snooping vlan 1 mrouter ethernet 1/11
Console(config)#
```

show ip igmp snooping mrouter

Use this command to display information on statically configured and dynamically learned multicast router ports.

Syntax

show ip igmp snooping mrouter [vlan *vlan-id*]

vlan-id - VLAN ID (Range: 1-4094)

Default Setting

Displays multicast router ports for all configured VLANs.

Command Mode

Privileged Exec

Command Usage

Multicast router port types displayed include Static or Dynamic.

Example

The following shows that port 11 in VLAN 1 is attached to a multicast router:

```

Console#show ip igmp snooping mrouter vlan 1
VLAN M'cast Router Ports Type
-----
    1                Eth 1/11  Static
    2                Eth 1/12  Dynamic
Console#

```

General Multicast Routing Commands

Command	Function	Mode	Page
ip multicast-routing	Enables IP multicast routing	GC	4-288
show ip mroute	Shows the IP multicast routing table	PE	4-288

ip multicast-routing

Use this command to enable IP multicast routing. Use the **no** form to disable IP multicast routing.

Syntax

ip multicast-routing
no ip multicast-routing

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

This command is used to enable multicast routing globally for the router. You also need to globally enable a specific multicast routing protocol using the **router dvmrp** or **router pim** command, and then specify the interfaces that will support multicast routing using the **ip dvmrp** or **ip pim dense-mode** commands.

Example

```
Console(config)#ip multicast-routing
Console(config)#
```

show ip mroute

Use this command to display the IP multicast routing table.

Syntax

show ip mroute [*group-address source*] [**summary**]

- *group-address* - An IP multicast group address with subscribers directly attached or downstream from this router.
- *source* - The IP subnetwork at the root of the multicast delivery tree. This subnetwork contains a known multicast source.
- **summary** - Displays summary information for each entry in the IP multicast routing table.

Command Mode

Privileged Exec

Command Usage

This command displays information for multicast routing. If no optional parameters are selected, detailed information for each entry in the multicast address table is displayed. If you select a multicast group and source pair, detailed information is displayed only for the specified entry. If the **summary** option is selected, an abbreviated list of information for each entry is displayed on a single line.

Example

This example shows detailed multicast information for a specified group/source pair

```

Console#show ip mroute 224.0.255.3 192.111.46.8
IP Multicast Forwarding is enabled.

IP Multicast Routing Table

Flags:  P - Prune, F - Forwarding
(192.111.46.0, 255.255.255.0, 224.0.255.3)
Owner:  DVMRP
Upstream Interface:  vlan1
Upstream Router:  148.122.34.9
Downstream:  vlan2(P), vlan3(F)
Console#

```

Field	Description
Source and netmask	Subnetwork containing the IP multicast source.
Group address	IP multicast group address for a requested service.
Owner	The associated multicast protocol (i.e., DVMRP or PIM-DM).
Upstream Interface	Interface leading to the upstream neighbor.
Upstream Router	IP address of the multicast router immediately upstream for this group.
Downstream interface and flags	The interface(s) on which multicast subscribers have been recorded. The flags associated with each interface indicate prune (P) if the downstream interface has been recently terminated or forwarding (F) if the interface is still active.

This example lists all entries in the multicast table in summary form:

```

Console#show ip mroute summary
IP Multicast Forwarding is enabled.

IP Multicast Routing Table (Summary)

Flags:  P - Prune UP

```

Group	Source	Source Mask	Interface	Owner	Flags
-----	-----	-----	-----	-----	-----
224.1.1.1	10.1.0.0	255.255.0.0	vlan1	DVMRP	P
224.2.2.2	10.1.0.0	255.255.0.0	vlan1	DVMRP	--

```

Console#

```

DVMRP Multicast Routing Commands

Command	Function	Mode	Page
router dvmrp	Enables DVMRP and enters router configuration mode	GC	4-291
probe-interval	Sets the interval for sending neighbor probe messages	RC	4-292
nbr-timeout	Sets the delay before declaring an attached neighbor router down	RC	4-293
report-interval	Sets the interval for propagating the complete set of routing tables to other neighbor routers	RC	4-293
flash-update-interval	Sets the interval for sending updates about changes to network topology	RC	4-294
prune-lifetime	Defines how long a prune state remains in effect for a source-routed multicast tree	RC	4-294
default-gateway	Configures the default gateway for IP multicast routing	RC	4-295
ip dvmrp	Enables DVMRP on the specified interface	IC	4-296
ip dvmrp metric	Sets the metric used when establishing reverse paths to some networks on directly attached interfaces	IC	4-297
clear ip dvmrp route	Clears all dynamic routes in the multicast routing table	PE	4-298
show router dvmrp	Displays global DVMRP configuration settings	NE, PE	4-298

Command	Function	Mode	Page
show ip dvmrp route	Displays DVMRP routing information	NE, PE	4-299
show ip dvmrp neighbor	Displays DVMRP neighbor information	NE, PE	4-300
show ip dvmrp interface	Displays DVMRP configuration settings for the interfaces	NE, PE	4-301

router dvmrp

Use this command to enable Distance-Vector Multicast Routing (DVMRP) globally for the router and to enter router configuration mode. Use the **no** form to disable DVMRP multicast routing.

Syntax

router dvmrp
no router dvmrp

Command Mode

Global Configuration

Command Usage

This command enables DVMRP globally for the router and enters router configuration mode. Make any changes necessary to the global DVMRP parameters. Then specify the interfaces that will support DVMRP multicast routing using the **ip dvmrp** command, and set the metric for each interface.

Example

```
Console(config)#router dvmrp
Console(config-router)#end
Console#show router dvmrp
Admin Status                : enable
Probe Interval              : 10
Nbr expire                  : 35
Minimum Flash Update Interval : 5
prune lifetime              : 7200
route report                 : 60
Default Gateway              : 0.0.0.0
Metric of Default Gateway   : 0
Console#
```

Related Commands

ip dvmrp (4-296)
show router dvmrp (4-298)

probe-interval

Use this command to set the interval for sending neighbor probe messages to the multicast group address for all DVMRP routers. Use the **no** form to restore the default value.

Syntax

probe-interval *seconds*
seconds - Interval between sending neighbor probe messages.
(Range: 1-65535)

Default Setting

10 seconds

Command Mode

Router Configuration

Command Usage

Probe messages are sent to neighboring DVMRP routers from which this device has received probes, and is used to verify whether or not these neighbors are still active members of the multicast tree.

Example

```
Console(config-router)#probe-interval 30  
Console(config-router)#
```

nbr-timeout

Use this command to set the interval to wait for messages from a DVMRP neighbor before declaring it dead. Use the **no** form to restore the default value.

Syntax

nbr-timeout *seconds*

seconds - Interval before declaring a neighbor dead. (Range: 1-65535)

Default Setting

35 seconds

Command Mode

Router Configuration

Command Usage

This command is used for timing out routes, and for setting the children and leaf flags.

Example

```
Console(config-router)#nbr-timeout 40
Console(config-router)#
```

report-interval

Use this command to specify how often to propagate the complete set of routing tables to other neighbor DVMRP routers. Use the **no** form to restore the default value.

Syntax

report-interval *seconds*

seconds - Interval between sending the complete set of routing tables. (Range: 1-65535)

Default Setting

60 seconds

Command Mode

Router Configuration

Example

```
Console(config-router)#report-interval 90
Console(config-router)#
```

flash-update-interval

Use this command to specify how often to send trigger updates, which reflect changes in the network topology. Use the **no** form to restore the default value.

Syntax

flash-update-interval *seconds*

seconds - Interval between sending flash updates when network topology changes have occurred. (Range: 1-65535)

Default Setting

5 seconds

Command Mode

Router Configuration

Example

```
Console(config-router)#flash-update-interval 10
Console(config-router)#
```

prune-lifetime

Use this command to specify how long a prune state will remain in effect for a multicast tree. Use the **no** form to restore the default value.

Syntax

prune-lifetime *seconds*

seconds - Prune state lifetime. (Range: 1-65535)

Default Setting

7200 seconds

Command Mode

Router Configuration

Command Usage

This command sets the prune state lifetime. After the prune state expires, the router will resume flooding multicast traffic from the multicast source device.

Example

```
Console(config-router)#prune-lifetime 5000
Console(config-router)#
```

default-gateway

Use this command to specify the default DVMRP gateway for IP multicast traffic. Use the **no** form to remove the default gateway.

Syntax

default-gateway *ip-address*

no default-gateway

ip-address - IP address of the default DVMRP gateway.

Default Setting

None

Command Mode

Router Configuration

Command Usage

- The specified interface advertises itself as a default route to neighboring DVMRP routers. It advertises the default route out through its other interfaces. Neighboring routers on the other interfaces return Poison Reverse messages for the default route back

to the router. When the router receives these messages, it records all the downstream routers for the default route.

- When multicast traffic with an unknown source address (i.e., not found in the route table) is received on the default upstream route interface, the router forwards this traffic out through the other interfaces (with known downstream routers). However, when multicast traffic with an unknown source address is received on another interface, the router drops it because only the default upstream interface can forward multicast traffic from an unknown source.

Example

```
Console(config-router)#default-gateway 10.1.0.253
Console(config-router)#
```

ip dvmrp

Use this command to enable DVMRP on the specified interface. Use the **no** form to disable DVMRP on this interface.

Syntax

ip dvmrp
no ip dvmrp

Default Setting

Disabled

Command Mode

Interface Configuration (VLAN)

Command Usage

To fully enable DVMRP, you need to enable multicast routing globally for the router with the **ip multicast-routing** command (page 4-288), enable DVMRP globally for the router with the **router dvmrp** command (page 4-291), and also enable DVMRP for each interface that will participate in multicast routing with the **ip dvmrp** command.

Example

```
Console(config)#interface vlan 1
Console(config-if)#ip dvmrp
Console(config-if)#end
Console#show ip dvmrp interface
Vlan 1 is up
    DVMRP is enabled
    Metric is 1
Console#
```

ip dvmrp metric

Use this command to configure the metric used in selecting the reverse path to networks connected directly to an interface on this router. Use the **no** form to restore the default value.

Syntax

ip dvmrp metric *interface-metric*
no ip dvmrp metric

interface-metric - Metric used to select the best reverse path.
(Range: 1-31)

Default Setting

1

Command Mode

Interface Configuration (VLAN)

Command Usage

The DVMRP interface metric is used to choose the best reverse path when there are multiple paths to the same upstream destination. The lower cost path is the preferred path.

Example

```
Console(config)#interface vlan 1
Console(config-if)#ip dvmrp metric 2
Console(config-if)#
```

clear ip dvmrp route

Use this command to clear all dynamic routes learned by DVMRP.

Command Mode

Privileged Exec

Example

As shown below, this command clears everything from the route table except for the default route.

Console#clear ip dvmrp route
clear all ip dvmrp route
Console#show ip dvmrp route

Source	Mask	Upstream_nbr	Interface	Metric	UpTime	Expire
10.1.0.0	255.255.255.0	10.1.0.253	vlan1	1	1840	0

Console#

show router dvmrp

Use this command to display the global DVMRP configuration settings.

Command Mode

Normal Exec, Privileged Exec

Command Usage

This command displays the global DVMRP settings described in the preceding pages:

- Admin Status, router dvmrp, (page 4-291)
- Probe Interval (page 4-292)
- Nbr Expire (page 4-293)
- Minimum Flash Update Interval (page 4-294)
- Prune Lifetime (page 4-294)
- Route Report (page 4-293)
- Default Gateway (page 4-295)
- Metric of Default Gateway (page 4-297)

Example

The default settings are shown in the following example:

```

Console#show route dvmrp
Admin Status           : enable
Probe Interval         : 10
Nbr expire             : 35
Minimum Flash Update Interval : 5
prune lifetime         : 7200
route report           : 60
Default Gateway        : 0.0.0.0
Metric of Default Gateway : 1
Console#
  
```

show ip dvmrp route

Use this command to display all entries in the DVMRP routing table.

Command Mode

Normal Exec, Privileged Exec

Example

DMVRP routes are shown in the following example:

```

Console#show ip dvmrp route

      Source           Mask           Upstream_nbr   Interface Metric UpTime Expire
-----
      10.1.0.0         255.255.255.0   10.1.0.253    vlan1      1   84438    0
      10.1.1.0         255.255.255.0   10.1.1.253    vlan2      1   84987    0
      10.1.8.0         255.255.255.0   10.1.0.254    vlan1      2   19729    97
Console#
  
```

Field	Description
Source	IP subnetwork that contains a multicast source, an upstream router, or an outgoing interface connected to multicast hosts.
Mask	Subnet mask that is used for the source address. This mask identifies the host address bits used for routing to specific subnets.
Upstream_nbr	The IP address of the network device immediately upstream for one or more multicast groups.
Interface	The IP interface on this router that connects to the upstream neighbor.
Metric	The metric for this interface used to calculate distance vectors.

Field	Description
UpTime	The time elapsed since this entry was created.
Expire	The time remaining before this entry will be aged out.

show ip dvmrp neighbor

Use this command to display all of the DVMRP neighbor routers.

Command Mode

Normal Exec, Privileged Exec

Example

Console#show ip dvmrp neighbor				
Address	Interface	Uptime	Expire	Capabilities
-----	-----	-----	-----	-----
10.1.0.254	vlan1	79315	32	6
Console#				

Field	Description
Address	The IP address of the network device immediately upstream for this multicast delivery tree.
Interface	The IP interface on this router that connects to the upstream neighbor.
Uptime	The time since this device last became a DVMRP neighbor.
Expire	The time remaining before this entry will be aged out.
Capabilities	The neighboring router's capabilities may include: Leaf (bit 0) - Neighbor has only one interface with neighbors. Prune (bit 1) - Neighbor supports pruning. Generation ID (bit 2) - Neighbor sends its Generation ID in probe messages. Mtrace (bit 3) - Neighbor can handle multicast trace requests. SNMP (bit 4) - Neighbor is SNMP capable. Netmask - (bit 5) - Neighbor will accept network masks appended to the prune, graft, and graft acknowledgement messages. Reserved (bit 6 and 7) - Reserved for future use.

show ip dvmrp interface

Use this command to display the DVMRP configuration for interfaces which have enabled DVMRP.

Command Mode

Normal Exec, Privileged Exec

Example

```
Console#show ip dvmrp interface
Vlan 1 is up
  DVMRP is enabled
  Metric is 1
Console#
```

PIM-DM Multicast Routing Commands

Command	Function	Mode	Page
router pim	Enables PIM globally for the router	GC	4-302
ip pim dense-mode	Enables PIM on the specified interface	IC	4-303
ip pim hello-interval	Sets the interval between sending PIM hello messages	IC	4-304
ip pim hello-holdtime	Sets the time to wait for hello messages from a neighboring PIM router before declaring it dead	IC	4-305
ip pim trigger-hello-interval	Sets the maximum time before sending a triggered PIM Hello message	IC	4-305
ip pim join-prune-holdtime	Configures the hold time for the prune state	IC	4-306
ip pim graft-retry-interval	Configures the time to wait for a Graft acknowledgement before resending a Graft message	IC	4-307
ip pim max-graft-retries	Configures the maximum number of times to resend a Graft message if it has not been acknowledged	IC	4-308
show router pim	Displays the global PIM configuration settings	NE, PE	4-308

Command	Function	Mode	Page
show ip pim interface	Displays information about interfaces configured for PIM	NE, PE	4-309
show ip pim neighbor	Displays information about PIM neighbors	NE, PE	4-309

router pim

Use this command to enable Protocol-Independent Multicast - Dense Mode (PIM-DM) globally for the router and to enter router configuration mode. Use the **no** form to disable PIM-DM multicast routing.

Syntax

router pim
no router pim

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

This command enables PIM-DM globally for the router. You also need to enable PIM-DM for each interface that will support multicast routing using the **ip pim dense-mode** command (page 4-303), and make any changes necessary to the multicast protocol parameters.

Example

```
Console(config)#router pim
Console#show router pim
Admin Status: Enabled
Console#
```

ip pim dense-mode

Use this command to enable PIM-DM on the specified interface. Use the **no** form to disable PIM-DM on this interface.

Syntax

```
ip pim dense-mode  
no pim dense-mode
```

Default Setting

Disabled

Command Mode

Interface Configuration (VLAN)

Command Usage

- To fully enable PIM-DM, you need to enable multicast routing globally for the router with the **ip multicast-routing** command (page 4-288), enable PIM-DM globally for the router with the **router pim** command (page 4-302), and also enable PIM-DM for each interface that will participate in multicast routing with the **ip pim dense-mode** command.
- If you enable PIM on an interface, you should also enable IGMP on that interface.
- Dense-mode interfaces are subject to multicast flooding by default, and are only removed from the multicast routing table when the router determines that there are no group members or downstream routers, or when a prune message is received from a downstream router.

Example

```
Console(config)#interface vlan 1
Console(config-if)#ip pim dense-mode
Console#show ip pim interface
Vlan 1 is up
  PIM is enabled, mode is Dense.
  Internet address is 10.1.0.253.
  Hello time interval is 30 sec, trigger hello time interval is 5 sec.
  Hello holdtime is 105 sec.
  Join/Prune holdtime is 210 sec.
  Graft retry interval is 3 sec, max graft retries is 2.
  DR Internet address is 10.1.0.253, neighbor count is 0.

Console#
```

ip pim hello-interval

Use this command to configure the frequency at which PIM hello messages are transmitted. Use the **no** form to restore the default value.

Syntax

ip pim hello-interval *seconds*

no ip pim hello-interval

seconds - Interval between sending PIM hello messages.
(Range: 1-65535)

Default Setting

30 seconds

Command Mode

Interface Configuration (VLAN)

Command Usage

Hello messages are sent to neighboring PIM routers from which this device has received probes, and are used to verify whether or not these neighbors are still active members of the multicast tree.

Example

```
Console(config-if)#ip pim hello-interval 60
Console(config-if)#
```

ip pim hello-holdtime

Use this command to configure the interval to wait for hello messages from a neighboring PIM router before declaring it dead. Use the **no** form to restore the default value.

Syntax

ip pim hello-holdtime *seconds*

no ip pim hello-holdtime

seconds - The hold time for PIM hello messages. (Range: 1-65535)

Default Setting

105 seconds

Command Mode

Interface Configuration (VLAN)

Command Usage

The **ip pim hello-holdtime** should be 3.5 times the value of **ip pim hello-holdtime** (page 4-304).

Example

```
Console(config-if)#ip pim hello-holdtime 210
Console(config-if)#
```

ip pim trigger-hello-interval

Use this command to configure the maximum time before transmitting a triggered PIM Hello message after the router is rebooted or PIM is enabled on an interface. Use the **no** form to restore the default value.

Syntax

ip pim trigger-hello-interval *seconds*

no ip pim trigger-hello-interval

seconds - The maximum time before sending a triggered PIM Hello message. (Range: 0-65535)

Default Setting

5 seconds

Command Mode

Interface Configuration (VLAN)

Command Usage

- When a router first starts or PIM is enabled on an interface, the hello-interval is set to random value between 0 and the trigger-hello-interval. This prevents synchronization of Hello messages on multi-access links if multiple routers are powered on simultaneously.
- Also, if a Hello message is received from a new neighbor, the receiving router will send its own Hello message after a random delay between 0 and the trigger-hello-interval.

Example

```
Console(config-if)#ip pim trigger-hello-interval 10
Console(config-if)#
```

ip pim join-prune-holdtime

Use this command to configure of the hold time for the prune state. Use the **no** form to restore the default value.

Syntax

ip pim join-prune-holdtime *seconds*

no ip pim join-prune-holdtime

seconds - The hold time for the prune state. (Range: 0-65535)

Default Setting

210 seconds

Command Mode

Interface Configuration (VLAN)

Command Usage

The multicast interface that first receives a multicast stream from a particular source forwards this traffic to all other PIM interfaces on the router. If there are no requesting groups on that interface, the leaf node sends a prune message upstream and enters a prune state for this multicast stream. The prune state is maintained until the join-prune-holdtime timer expires or a graft message is received for the forwarding entry.

Example

```
Console(config-if)#ip pim join-prune-holdtime 60
Console(config-if)#
```

ip pim graft-retry-interval

Use this command to configure the time to wait for a Graft acknowledgement before resending a Graft. Use the **no** form to restore the default value.

Syntax

ip pim graft-retry-interval *seconds*
no ip pim graft-retry-interval

seconds - The time before resending a Graft. (Range: 0-65535)

Default Setting

3 seconds

Command Mode

Interface Configuration (VLAN)

Command Usage

A graft message is sent by a router to cancel a prune state. When a router receives a graft message, it must respond with an graft acknowledgement message. If this acknowledgement message is lost, the router that sent the graft message will resend it a number of times (as defined by the **ip pim max-graft-retries** command).

Example

```
Console(config-if)#ip pim graft-retry-interval 9
Console(config-if)#
```

ip pim max-graft-retries

Use this command to configure the maximum number of times to resend a Graft message if it has not been acknowledged. Use the **no** form to restore the default value.

Syntax

ip pim max-graft-retries *retries*
no ip pim graft-retry-interval

retries - The maximum number of times to resend a Graft.
(Range: 0-65535)

Default Setting

2

Command Mode

Interface Configuration (VLAN)

Example

```
Console(config-if)#ip pim max-graft-retries 5
Console(config-if)#
```

show router pim

Use this command to display the global PIM configuration settings.

Command Mode

Normal Exec, Privileged Exec

Example

```
Console#show router pim
Admin Status: Enabled
Console#
```

show ip pim interface

Use this command to display information about interfaces configured for PIM.

Syntax

show ip pim interface *vlan-id*
vlan-id - VLAN ID (Range: 1-4094)

Command Mode

Normal Exec, Privileged Exec

Command Usage

This command displays the PIM settings for the specified interface as described in the preceding pages. It also shows the address of the designated PIM router and the number of neighboring PIM routers.

Example

```
Console#show ip pim interface 1
Vlan 1 is up
PIM is enabled, mode is Dense.
Internet address is 10.1.0.253.
Hello time interval is 30 sec, trigger hello time interval is 5 sec.
Hello holdtime is 105 sec.
Join/Prune holdtime is 210 sec.
Graft retry interval is 3 sec, max graft retries is 2.
DR Internet address is 10.1.0.254, neighbor count is 1.

Console#
```

show ip pim neighbor

Use this command to display information about PIM neighbors.

Syntax

show ip pim neighbor [*ip-address*]
ip-address - IP address of a PIM neighbor.

Default Setting

Displays information for all known PIM neighbors.

Command Mode

Normal Exec, Privileged Exec

Example

```
Console#show ip pim neighbor
      Address      VLAN Interface  Uptime    Expire    Mode
-----
      10.1.0.254      1      17:38:16  00:01:25  Dense
Console#
```

Field	Description
Address	IP address of the next-hop router.
VLAN Interface	Interface number that is attached to this neighbor.
Uptime	The duration this entry has been active.
Expire	The time before this entry will be removed.
Mode	PIM mode used on this interface. (Only Dense Mode is supported.)

APPENDIX A

TROUBLESHOOTING

Troubleshooting Chart	
Symptom	Action
Cannot connect using Telnet, Web browser, or SNMP software	<ul style="list-style-type: none">• Be sure you have configured the agent with a valid IP address, subnet mask and default gateway.• If you are trying to connect to the agent via the IP address for a tagged VLAN group, your management station must include the appropriate tag in its transmitted frames.• Check that you have a valid network connection to the switch and that the port you are using has not been disabled.• Check network cabling between the management station and the switch.• If you cannot connect using Telnet, you may have exceeded the maximum number of concurrent Telnet sessions permitted. Try connecting again at a later time.
Cannot access the on-board configuration program via a serial port connection	<ul style="list-style-type: none">• Be sure you have set the terminal emulator program to VT100 compatible, 8 data bits, 1 stop bit, no parity and 9600 bps.• Check that the null-modem serial cable conforms to the pin-out connections provided in Appendix B.
Forgot or lost the password	<ul style="list-style-type: none">• Reinstall the switch defaults. Make a direct connection to the switch's console port and power cycle the switch. Immediately after powering on, press <Ctrl><u> to access the system file menu. Select <D> to delete all user-defined configuration files. Press <Q> to boot the switch.

APPENDIX B

UPGRADING FIRMWARE VIA THE SERIAL PORT

The switch contains three firmware components that can be upgraded; the loader code, diagnostics (or Boot-ROM) code, and runtime operation code. The runtime code can be upgraded via the switch's RS-232 serial console port, via a network connection to a TFTP server, or using SNMP management software. The loader code and diagnostics code can be upgraded only via the switch's RS-232 serial console port.

Note: You can use the switch's web interface to download runtime code via TFTP. Downloading large runtime code files via TFTP is normally much faster than downloading via the switch's serial port.

You can upgrade switch firmware by connecting a PC directly to the serial Console port on the switch's front panel and using VT100 terminal emulation software that supports the XModem protocol. (See "Required Connections" on page 2-2.)

1. Connect a PC to the switch's Console port using a null-modem or crossover RS-232 cable with a female DB-9 connector.
2. Configure the terminal emulation software's communication parameters to 9600 baud, 8 data bits, 1 stop bit, no parity, and set flow control to *none*.
3. Power cycle the switch.
4. When the switch initialization screen appears, enter firmware-download mode by pressing <Ctrl><u> immediately after

power on or rebooting the switch. Screen text similar to that shown below displays:

File Name	S/Up	Type	Size	Create Time
-----	-----	-----	-----	-----
\$logfile_1	0	3	64	00:00:07
\$logfile_2	0	3	64	00:00:12
diag_0070	0	1	96500	00:06:37
diag_0074	1	1	97780	00:00:05
run_03024	0	2	1121956	00:21:41
run_10020	1	2	1124416	00:00:10
-----	-----	-----	-----	-----
[X]modem Download [D]elete File [S]et Startup File				
[R]eturn to Factory Default [C]hange Baudrate [Q]uit				
Select>				

5. Press <c> to change the baud rate of the switch's serial connection.
6. Press to select the option for 115200 baud.
7. There are two baud rate settings available, 9600 and 115200. Using the higher baud rate minimizes the time required to download firmware code files.
8. Set your PC's terminal emulation software to match the 115200 baud rate. Press <Enter> to reset communications with the switch.

```
Select>
Change baudrate [A]9600 [B]115200
Baudrate set to 115200
```

9. Check that the switch has sufficient flash memory space for the new code file before starting the download.
10. You can store a maximum of only two runtime and two diagnostic code files in the switch's flash memory. Use the **[D]elete File** command to remove a runtime or diagnostic file.
11. Press <x> to start downloading the new code file.

12. If using Windows HyperTerminal, click the “Transfer” button, and then click “Send File...” Select the XModem Protocol and then use the “Browse” button to select the required firmware code file from your PC system. The “Xmodem file send” window displays the progress of the download procedure.

Note: The download file must be a binary software file for this switch.

13. After the file has been downloaded, you are prompted with “Update Image File:” to specify the type of code file. Press <R> for runtime code, <D> for diagnostic code, or <L> for loader code.

Note: If you select <L> for loader code, be sure the file is a valid loader code file for the switch. If you download an invalid file, the switch will not be able to boot. Unless absolutely necessary, do not attempt to download loader code files.

14. Specify a name for the downloaded code file. File names are case-sensitive, should be from 1 to 31 characters, not contain slashes (\ or /), and the leading letter of the file name should not be a period (.). (Valid characters: A-Z, a-z, 0-9, “.”, “-”, “_”)
15. For example, the following screen text shows the download procedure for a runtime code file:

```
Select>x
Xmodem Receiving Start ::
Image downloaded to buffer.

      [R]runtime
      [D]diagnostic
      [L]loader (Warning: you sure what you are doing?)
Update Image File:r
Runtime Image Filename : run_1013
Updating file system.
File system updated.
[Press any key to continue]
```

16. To set the new downloaded file as the startup file, use the **[S]et Startup File** menu option.
17. When you have finished downloading code files, use the **[C]hange Baudrate** menu option to change the baud rate of the switch's serial connection back to 9600 baud.
18. Set your PC's terminal emulation software baud rate back to 9600 baud. Press <Enter> to reset communications with the switch.
19. Press <q> to quit the firmware-download mode and boot the switch.

GLOSSARY

Access Control List (ACL)

ACLs can limit network traffic and restrict access to certain users or devices by checking each packet for certain IP or MAC (i.e., Layer 2) information.

Address Resolution Protocol (ARP)

ARP converts between IP addresses and MAC (i.e., hardware) addresses. ARP is used to locate the MAC address corresponding to a given IP address. This allows the switch to use IP addresses for routing decisions and the corresponding MAC addresses to forward packets from one hop to the next.

Boot Protocol (BOOTP)

BOOTP is used to provide bootup information for network devices, including IP address information, the address of the TFTP server that contains the devices system files, and the name of the boot file.

Class of Service (CoS)

CoS is supported by prioritizing packets based on the required level of service, and then placing them in the appropriate output queue. Data is transmitted from the queues using weighted round-robin service to enforce priority service and prevent blockage of lower-level queues. Priority may be set according to the port default, the packet's priority bit (in the VLAN tag), TCP/UDP port number, IP Precedence bit, or DSCP priority bit.

Differentiated Services Code Point Service (DSCP)

DSCP uses a six-bit tag to provide for up to 64 different forwarding behaviors. Based on network policies, different kinds of traffic can be marked for different kinds of forwarding. The DSCP bits are mapped to the Class of Service categories, and then into the output queues.

Distance Vector Multicast Routing Protocol (DVMRP)

A distance-vector-style routing protocol used for routing multicast datagrams through the Internet. DVMRP combines many of the features of RIP with Reverse Path Forwarding (RPF).

Dynamic Host Control Protocol (DHCP)

Provides a framework for passing configuration information to hosts on a TCP/IP network. DHCP is based on the Bootstrap Protocol (BOOTP), adding the capability of automatic allocation of reusable network addresses and additional configuration options.

Extensible Authentication Protocol over LAN (EAPOL)

EAPOL is a client authentication protocol used by this switch to verify the network access rights for any device that is plugged into the switch. A user name and password is requested by the switch, and then passed to an authentication server (e.g., RADIUS) for verification. EAPOL is implemented as part of the IEEE 802.1x Port Authentication standard.

GARP VLAN Registration Protocol (GVRP)

Defines a way for switches to exchange VLAN information in order to register necessary VLAN members on ports along the Spanning Tree so that VLANs defined in each switch can work automatically over a Spanning Tree network.

Generic Attribute Registration Protocol (GARP)

GARP is a protocol that can be used by endstations and switches to register and propagate multicast group membership information in a switched environment so that multicast data frames are propagated only to those parts of a switched LAN containing registered endstations. Formerly called Group Address Registration Protocol.

Generic Multicast Registration Protocol (GMRP)

GMRP allows network devices to register end stations with multicast groups. GMRP requires that any participating network devices or end stations comply with the IEEE 802.1p standard.

Group Attribute Registration Protocol (GARP)

See Generic Attribute Registration Protocol.

IEEE 802.1D

Specifies a general method for the operation of MAC bridges, including the Spanning Tree Protocol.

IEEE 802.1Q

VLAN Tagging—Defines Ethernet frame tags which carry VLAN information. It allows switches to assign endstations to different virtual LANs, and defines a standard way for VLANs to communicate across switched networks.

IEEE 802.1p

An IEEE standard for providing quality of service (QoS) in Ethernet networks. The standard uses packet tags that define up to eight traffic classes and allows switches to transmit packets based on the tagged priority value.

IEEE 802.1x

Port Authentication controls access to the switch ports by requiring users to first enter a user ID and password for authentication.

IEEE 802.3ac

Defines frame extensions for VLAN tagging.

IEEE 802.3x

Defines Ethernet frame start/stop requests and timers used for flow control on full-duplex links.

IGMP Snooping

Listening to IGMP Query and IGMP Report packets transferred between IP Multicast Routers and IP Multicast host groups to identify IP Multicast group members.

IGMP Query

On each subnetwork, one IGMP-capable device will act as the querier — that is, the device that asks all hosts to report on the IP multicast groups they wish to join or to which they already belong. The elected querier will be the device with the lowest IP address in the subnetwork.

Internet Control Message Protocol (ICMP)

A network layer protocol that reports errors in processing IP packets. ICMP is also used by routers to feed back information about better routing choices.

Internet Group Management Protocol (IGMP)

A protocol through which hosts can register with their local router for multicast services. If there is more than one multicast router on a given subnetwork, one of the routers is made the “querier” and assumes responsibility for keeping track of group membership.

In-Band Management

Management of the network from a station attached directly to the network.

IP Multicast Filtering

A process whereby this switch can pass multicast traffic along to participating hosts.

IP Precedence

The Type of Service (ToS) octet in the IPv4 header includes three precedence bits defining eight different priority levels ranging from highest priority for network control packets to lowest priority for routine traffic. The eight values are mapped one-to-one to the Class of Service categories by default, but may be configured differently to suit the requirements for specific network applications.

Layer 2

Data Link layer in the ISO 7-Layer Data Communications Protocol. This is related directly to the hardware interface for network devices and passes on traffic based on MAC addresses.

Layer 3

Network layer in the ISO 7-Layer Data Communications Protocol. This layer handles the routing functions for data moving from one open system to another.

Link Aggregation

See Port Trunk.

Link Aggregation Control Protocol (LACP)

Allows ports to automatically negotiate a trunked link with LACP-configured ports on another device.

Management Information Base (MIB)

An acronym for Management Information Base. It is a set of database objects that contains information about a specific device.

Multicast Switching

A process whereby the switch filters incoming multicast frames for services for which no attached host has registered, or forwards them to all ports contained within the designated multicast VLAN group.

Network Time Protocol (NTP)

NTP provides the mechanisms to synchronize time across the network. The time servers operate in a hierarchical-master-slave configuration in order to synchronize local clocks within the subnet and to national time standards via wire or radio.

Open Shortest Path First (OSPF)

OSPF is a link-state routing protocol that functions better over a larger network such as the Internet, as opposed to distance-vector routing protocols such as RIP. It includes features such as unlimited hop count, authentication of routing updates, and Variable Length Subnet Masks (VLSM).

Out-of-Band Management

Management of the network from a station not attached to the network.

Port Authentication

See IEEE 802.1x.

Port Mirroring

A method whereby data on a target port is mirrored to a monitor port for troubleshooting with a logic analyzer or RMON probe. This allows data on the target port to be studied unobstructively.

Port Trunk

Defines a network link aggregation and trunking method which specifies how to create a single high-speed logical link that combines several lower-speed physical links.

Private VLANs

Private VLANs provide port-based security and isolation between ports within the assigned VLAN. Data traffic on downlink ports can only be forwarded to, and from, uplink ports.

Protocol-Independent Multicasting (PIM)

This multicast routing protocol floods multicast traffic downstream, and calculates the shortest-path back to the multicast source network via reverse path forwarding. PIM uses the router's IP routing table rather than maintaining a separate multicast routing table as with DVMRP. PIM - Sparse Mode is designed for networks where the probability of a multicast client is low, such as on a Wide Area Network. PIM - Dense Mode is designed for networks where the probability of a multicast client is high and frequent flooding of multicast traffic can be justified.

Remote Authentication Dial-in User Service (RADIUS)

RADIUS is a logon authentication protocol that uses software running on a central server to control access to RADIUS-compliant devices on the network.

Remote Monitoring (RMON)

RMON provides comprehensive network monitoring capabilities. It eliminates the polling required in standard SNMP, and can set alarms on a variety of traffic conditions, including specific error types.

Rapid Spanning Tree Protocol (RSTP)

RSTP reduces the convergence time for network topology changes to about 10% of that required by the older IEEE 802.1D STP standard.

Routing Information Protocol (RIP)

The RIP protocol seeks to find the shortest route to another device by minimizing the distance-vector, or hop count, which serves as a rough estimate of transmission cost. RIP-2 is a compatible upgrade to RIP. It adds useful capabilities for subnet routing, authentication, and multicast transmissions.

Simple Network Management Protocol (SNMP)

The application protocol in the Internet suite of protocols which offers network management services.

Simple Network Time Protocol (SNTP)

SNTP allows a device to set its internal clock based on periodic updates from a Network Time Protocol (NTP) server. Updates can be requested from a specific NTP server, or can be received via broadcasts sent by NTP servers.

Spanning Tree Protocol (STP)

A technology that checks your network for any loops. A loop can often occur in complicated or backup linked network systems. Spanning Tree detects and directs data along the shortest available path, maximizing the performance and efficiency of the network.

Telnet

Defines a remote communication facility for interfacing to a terminal device over TCP/IP.

Transmission Control Protocol/Internet Protocol (TCP/IP)

Protocol suite that includes TCP as the primary transport protocol, and IP as the network layer protocol.

Trivial File Transfer Protocol (TFTP)

A TCP/IP protocol commonly used for software downloads.

User Datagram Protocol (UDP)

UDP provides a datagram mode for packet-switched communications. It uses IP as the underlying transport mechanism to provide access to IP-like services. UDP packets are delivered just like IP packets – connection-less datagrams that may be discarded before reaching their targets. UDP is useful when TCP would be too complex, too slow, or just unnecessary.

Virtual LAN (VLAN)

A Virtual LAN is a collection of network nodes that share the same collision domain regardless of their physical location or connection point in the network. A VLAN serves as a logical workgroup with no physical barriers, and allows users to share information and resources as though located on the same LAN.

XModem

A protocol used to transfer files between devices. Data is grouped in 128-byte blocks and error-corrected.

INDEX

A

acceptable frame type 3-115, 4-167

Access Control List *See* ACL

ACL

Extended IP 3-42, 4-75, 4-76, 4-79

MAC 3-42, 4-75, 4-84, 4-84–4-88

Standard IP 3-42, 4-75, 4-76, 4-78

Address Resolution Protocol *See* ARP

address table 3-84, 4-141

aging time 3-87, 4-145

ARP

configuration 3-159, 4-221

description 3-157

proxy 3-158, 4-224

statistics 3-164, 4-229

B

BOOTP 3-20, 4-216

BPDU 3-88

broadcast storm, threshold 3-69, 4-126

C

Class of Service *See* CoS

CLI, showing commands 4-5

command line interface *See* CLI

community string 2-9, 3-50, 4-90

configuration settings, saving or

restoring 2-11, 3-23, 4-53

console port, required connections 2-2

CoS

configuring 3-120, 4-181

copying settings 3-133

DSCP 3-129, 4-191

IP port priority 3-131, 4-187

IP precedence 3-127, 4-189

layer 3/4 priorities 3-125, 4-187

queue mapping 3-122, 4-184

traffic class weights 3-124, 4-183

D

default gateway, configuration 3-154,
4-218

default priority, ingress port 3-120, 4-182

default settings, system 1-8

DHCP 3-20, 4-216

address pool 3-57, 4-104

client 3-18, 4-97

dynamic configuration 2-8

relay service 3-53, 4-99

server 3-55, 4-102

Differentiated Code Point Service *See*
DSCP

downloading software 3-22, 4-53, B-1

DSCP

enabling 3-126, 4-191

mapping priorities 3-129, 4-191

DVMRP

configuring 3-222, 4-290

global settings 3-223, 4-290–4-295

interface settings 3-227, 4-296–4-297

neighbor routers 3-229, 4-300

routing table 3-230, 4-299

dynamic addresses, displaying 3-85, 4-143

Dynamic Host Configuration Protocol *See*
DHCP

E

edge port, STA 3-97, 3-101, 4-156

event logging 4-37

F

firmware

- displaying version 3-14, 4-52
- upgrading 3-22, 4-53, B-1

G

GARP VLAN Registration Protocol *See*
GVRP

gateway, default 3-154, 4-218

GVRP

- global setting 3-107, 4-175
- interface configuration 3-115, 4-177

H

hardware version, displaying 3-14, 4-52

I

IEEE 802.1D 3-87, 4-148

IEEE 802.1w 3-87, 4-148

IEEE 802.1x 3-32, 4-66

IEEE 802.1x, port authentication 3-32,
4-66

IGMP

- description of protocol 3-135
- groups, displaying 3-142, 4-213
- Layer 2 3-136, 4-196
- Layer 3 3-144, 4-205
- query 3-136, 4-201, 4-206
- query, Layer 2 3-137, 4-201
- query, Layer 3 3-144, 4-205
- services, displaying 3-148, 4-213
- snooping 3-136, 4-197
- snooping, configuring 3-137, 4-196
- ingress filtering 3-115, 4-168
- IP address

- BOOTP/DHCP 3-20, 4-98, 4-216
- setting 2-6, 3-17, 4-216

IP port priority

- enabling 3-131, 4-187
- mapping priorities 3-131, 4-188

IP precedence

- enabling 3-126, 4-189
- mapping priorities 3-127, 4-189

IP routing 3-149, 4-225

- configuring interfaces 3-155, 4-216
- enabling or disabling 3-154, 4-226
- status 3-154, 4-226
- unicast protocols 3-152

IP, statistics 3-165, 4-229

L

link type, STA 3-98, 3-101, 4-158

log-in, Web interface 3-3

logon authentication 3-28, 4-60

- RADIUS client 3-30, 4-61

- RADIUS server 3-30, 4-61

logon authentication, sequence 3-31,
4-60

M

main menu 3-5

mirror port, configuring 3-70, 4-133

multicast filtering 3-134, 4-196

multicast groups 3-142, 3-148, 4-200

- displaying 3-148, 4-200

- static 3-142, 4-197

multicast routing 3-218, 4-285

- description 3-218

- DVMRP 3-222, 4-290

- enabling 3-219, 4-288

- general commands 4-287

- global settings 3-219, 4-288

- PIM-DM 3-231, 4-301

- routing table 3-219, 4-288
- multicast services
 - configuring 3-143, 4-197
 - displaying 3-142, 4-200
- multicast, static router port 3-140, 4-286

O

- OSPF 3-186, 4-244
 - area border router 3-189, 4-251
 - AS summary route 3-208, 4-253
 - autonomous system boundary
 - router 3-189, 4-249
 - backbone 3-192, 4-256
 - default external route 3-190, 4-248
 - general settings 3-188, 4-244
 - normal area 3-192, 4-255
 - NSSA 3-192, 4-258
 - redistributing external routes 3-210, 4-254
 - stub 3-192, 4-257
 - transit area 3-192, 4-260
 - virtual link 3-204, 4-260

P

- password, line 4-16
- passwords 2-6
 - administrator setting 3-28, 4-33
- path cost 3-97
 - method 3-94, 4-152
 - STA 3-97, 4-152
- PIM-DM 3-231, 4-301
 - configuring 3-231, 4-301
 - global configuration 3-232, 4-302
 - interface settings 3-233, 4-303—4-308
 - neighbor routers 3-237, 4-309
- port authentication 3-32, 4-66
- port priority
 - configuring 3-120, 4-181

- default ingress 3-120, 4-182
- STA 3-97, 4-155
- port, statistics 3-71, 4-129
- ports
 - autonegotiation 3-67, 4-121
 - broadcast storm threshold 3-69, 4-126
 - capabilities 3-67, 4-122
 - duplex mode 3-67, 4-120
 - flow control 3-67, 4-124
 - speed 3-67, 4-120
- ports, configuring 3-63, 4-118
- ports, mirroring 3-70, 4-133
- priority, default port ingress 3-120, 4-182
- problems, troubleshooting A-1
- protocol migration 3-101, 4-159
- proxy ARP 3-158, 4-224

Q

- queue weights 3-124, 4-183

R

- RADIUS, logon authentication 3-30, 4-61
- rate limits, setting 3-77, 4-135
- restarting the system 3-28, 4-28
- RIP
 - configuring 3-175, 4-231—4-242
 - description 3-153
 - global settings 3-176, 4-231—4-232
 - interface protocol settings 3-179, 4-233—4-241
 - specifying interfaces 3-178, 4-233
 - statistics 3-183, 4-243
- routing table, displaying 3-173, 4-228
- RSTP 3-87, 4-148
 - global configuration 3-89, 4-148

S

serial port

- configuring 4-13

- XModem downloads B-1

Simple Network Management Protocol *See* SNMP

SNMP 3-50

- community string 3-50, 4-90

- enabling traps 3-51, 4-94

- trap manager 3-51, 4-93

software

- displaying version 3-14, 4-52

- downloading 3-22, 4-53, B-1

Spanning Tree Protocol *See* STA

STA 3-87, 4-146

- edge port 3-97, 3-101, 4-156

- global settings, configuring 3-92, 4-147–4-153

- global settings, displaying 3-89, 4-160

- interface settings 3-95, 4-154–4-159, 4-160

- link type 3-98, 3-101, 4-158

- path cost 3-97, 4-154

- path cost method 3-94, 4-152

- port priority 3-97, 4-155

- protocol migration 3-101, 4-159

- transmission limit 3-94, 4-153

startup files

- creating 3-24, 4-53

- displaying 3-22, 4-47

- setting 3-22, 4-59

static addresses, setting 3-84, 4-141

static routes, configuring 3-172, 4-227

statistics

- ARP 3-164, 4-229

- ICMP 3-168, 4-229

- IP 3-165, 4-229

- port 3-71, 4-129

- RIP 3-183, 4-243

- TCP 3-171, 4-229

- UDP 3-170, 4-229

STP 3-92, 4-148

STP *Also see* STA

system clock, setting 3-25, 4-41

system software, downloading from server 3-22, 4-53

T

time, setting 3-25, 4-41

traffic class weights 3-124, 4-183

trap manager 2-11, 3-51, 4-93

troubleshooting A-1

trunk

- configuration 3-79, 4-137

- LACP 3-80, 4-139

- static 3-82, 4-138

U

upgrading software 3-22, 4-53, B-1

user password 3-28, 4-33, 4-34

V

VLANs 3-102–3-119, 4-162–4-174

- adding static members 3-111, 3-113, 4-170

- creating 3-110, 4-163

- description 3-102

- displaying basic information 3-107, 4-176

- displaying port members 3-108, 4-172

- egress mode 3-116, 4-166

- interface configuration 3-114, 4-167–4-171

- private 3-118, 4-173

W

Web interface

- access requirements 3-1
- configuration buttons 3-4
- home page 3-3

menu list 3-5

panel display 3-4

X

XModem downloads B-1

INDEX

FOR TECHNICAL SUPPORT, CALL:

From U.S.A. and Canada (24 hours a day, 7 days a week)

(800) SMC-4-YOU; Phn: (949) 679-8000; Fax: (949) 679-1481

From Europe Contact details can be found on

www.smc-europe.com or www.smc.com

INTERNET

E-mail addresses:

techsupport@smc.com

european.techsupport@smc-europe.com

Driver updates:

http://www.smc.com/index.cfm?action=tech_support_drivers_downloads

World Wide Web:

<http://www.smc.com>

<http://www.smc-europe.com>

FOR LITERATURE OR ADVERTISING RESPONSE, CALL:

U.S.A. and Canada:	(800) SMC-4-YOU	Fax (949) 679-1481
Spain:	34-91-352-00-40	Fax 34-93-477-3774
UK:	44 (0) 1932 866553	Fax 44 (0) 118 974 8701
France:	33 (0) 41 38 32 32	Fax 33 (0) 41 38 01 58
Italy:	39 (0) 3355708602	Fax 39 02 739 14 17
Benelux:	31 33 455 72 88	Fax 31 33 455 73 30
Central Europe:	49 (0) 89 92861-0	Fax 49 (0) 89 92861-230
Nordic:	46 (0) 868 70700	Fax 46 (0) 887 62 62
Eastern Europe:	34 -93-477-4920	Fax 34 93 477 3774
Sub Saharian Africa:	216-712-36616	Fax 216-71751415
North West Africa:	34 93 477 4920	Fax 34 93 477 3774
CIS:	7 (095) 7893573	Fax 7 (095) 789 357
PRC:	86-10-6235-4958	Fax 86-10-6235-4962
Taiwan:	886-2-87978006	Fax 886-2-87976288
Asia Pacific:	(65) 238 6556	Fax (65) 238 6466
Korea:	82-2-553-0860	Fax 82-2-553-7202
Japan:	81-45-224-2332	Fax 81-45-224-2331
Australia:	61-2-8875-7887	Fax 61-2-8875-7777
India:	91-22-8204437	Fax 91-22-8204443

If you are looking for further contact information, please visit www.smc.com,
www.smc-europe.com, or www.smc-asia.com.



38 Tesla
Irvine, CA 92618
Phone: (949) 679-8000

Model Number: SMC6724L3
Publication Number: 150200033700A
Revision Number: F1.2.0.4 E102003-R01